ALEJANDRO SUÁREZ SÁNCHEZ-OCAÑA

Autor del bestseller *"Desnudando a Google"*

# EL QUINTO ELEMENTO

## ESPIONAJE, CIBERGUERRA Y TERRORISMO. UNA AMENAZA REAL E INMINENTE




LA REALIDAD QUE TE ESTÁN OCULTANDO:
**EL PRÓXIMO 11-S EMPEZARÁ CON UN CLIC**

DEUSTO

# Índice

Portada
Citas
Dedicatoria
Introducción

1. ¿Cómo hemos llegado aquí? Un viaje por el tiempo
    Los papeles del Pentágono
    Wikileaks
    El caso Snowden

2. Espionaje económico e industrial
    Era «súper», pero no tenía superpoderes
    El amigo americano: ¡tener amigos para esto!
    El día que los chinos se colaron hasta la cocina en Alcobendas
    Oh là là: la maldición del último euro
    Cuando los malos fueron los buenos
    El ataque que cambió tu tarjeta de crédito
    El gran negocio del espionaje tecnológico
    El floreciente mercado de los zero days
    El cazador cazado
    Silicon Valley, la sede de esos brillantes muchachos que trabajan para la NSA
    Así leen los amigos de la NSA tu correo electrónico
    Nadie le regala a Obama un iPhone por Navidad

3. Cibercrimen
    ¿Qué demonios es eso del cibercrimen?

Cuando el progreso se nos va de las manos
Entonces, ¿Bin Laden era un emprendedor?
Hacktivistas
El lado oscuro de la red: la darknet
Cosas de locos que lo flipas
Las Páginas Amarillas del cibercrimen
Estafas digitales

4. Ciberterrorismo
Una amenaza muy real
La tecnología, ¿amiga o enemiga?
El contraterrorismo también tiene ordenadores
Ojo: ¡qué te la cuelan por Detroit!
Reclutando imbéciles
Chateando con el enemigo
Financiación del terrorismo en internet
Aprendiz de 007

5. Ciberguerra
La guerra no es un juego, chavalote
Cisnes negros
Una guerra sin tiros
Tiempos modernos, guerras modernas
Guerra 3.0
Estados Unidos vs. China
Hackers patrióticos: unos «motivados» del sistema
Desde Rusia, con amor
Bombas digitales, ¿bombas reales?
Hay un gusano en mi manzana
Tres, dos, uno…, zero days
La respuesta está… ¡en la Biblia!
El país de Anacleto, agente secreto, y la ciberguerra
Me cago en la mar
Una nueva carrera de armamentos
El fantasma de la guerra fría
Si un ataque no está definido, no hay respuesta

Amenazas y ataques preventivos
Incertidumbre y estrategia digitales
La ciberdefensa de la OTAN

6. ¡Gracias, tecnología, por convertirnos en un saco de boxeo!
Un sistema de localización que, además, sirve para hablar por teléfono
Págate una conexión, no seas cutre…, ¡o sufre las consecuencias!
Pero yo estoy protegido porque uso TOR y cifro mis discos duros
Un dron con Antrax como regalo de cumpleaños
Como en Minority Report, pero sin Tom Cruise

7. Controla el código y controlarás el mundo
¿Y si el futuro fuera como en Mad Max?
El futuro ya está aquí, y no era exactamente lo que esperábamos
La trampa tecnológica
El crimen es como un juego de niños, pero con adultos
Los crímenes de mañana, en los periódicos de ayer
La ilusión democrática de internet
Internet de las cosas
Los riesgos de la hiperconectividad
Libertad vigilada
Póntelo, pónselo
Los rompecorazones (literalmente)
Bienvenidos a Gattaca
Por tu cara bonita
Biohacking
¿Smartcities o ciudades no tan inteligentes?
Las dos caras del progreso

Bibliografía
Notas
Créditos

## Te damos las gracias por adquirir este EBOOK

Visita **Planetadelibros.com** y descubre una nueva forma de disfrutar de la lectura

---

**¡Regístrate y accede a contenidos exclusivos!**

Próximos lanzamientos
Clubs de lectura con autores
Concursos y promociones
Áreas temáticas
Presentaciones de libros
Noticias destacadas

PlanetadeLibros.com

---

**Comparte tu opinión en la ficha del libro y en nuestras redes sociales:**

## Explora Descubre Comparte

*(Léase con voz de robot ochentero)*
Extraño juego. El único movimiento para ganar es no jugar.

*Juegos de guerra*, Metro Goldwyn Mayer, 1983

Aquellos que sacrifican libertad por seguridad, no merecen ni la una ni la otra.

BENJAMIN FRANKLIN

Con mi agradecimiento a Aurora Nacarino, Fernando Varela, al agente Klasus y a Roberto Ballesteros, sin los que no hubiera sido posible este libro.

Dedicado a José María *Batman*, Candela e Isabel, que me aguantan en el día a día.

Hago extensible la dedicatoria a todos los miembros de las fuerzas y cuerpos de seguridad del Estado,
que apenas intuyen los duros años que se les vienen encima.

A.

# Introducción

Dicen los científicos que nuestro sistema solar se formó hace unos 4.600 millones de años. En la Tierra, uno de sus planetas, la vida surgió unos 900 millones de años después, es decir, hace más de 3.700 millones de años.

Comparada con esas enormes cifras, la aparición del ser humano en la Tierra es relativamente reciente: se suele cifrar en hace «tan sólo» tres o cuatro millones de años.

Desde que comenzó la andadura de nuestra especie, los acontecimientos han ido adquiriendo velocidad a medida que los avances tecnológicos así lo han propiciado. Aunque hoy nos parezca increíble, todo empezó a ocurrir muy lentamente. En la actualidad podríamos estar tentados de creer que no estamos genéticamente preparados para entender cómo ha cambiado el mundo en tan breve espacio de tiempo. Podríamos afirmar sin rubor que, si una persona entrara en estado de coma y despertara unos pocos años después, el mundo habría cambiado para ella tan radical e incomprensiblemente que necesitaría un enorme periodo de aprendizaje y adaptación para volver a comprenderlo. El futuro ya no es lo que era.

Desde que los primeros humanos habitaron nuestro planeta hace miles de años, parecía que apenas pasaba nada. De hecho, podríamos relacionar el primer punto de inflexión de nuestra evolución social con un gran invento cuyo desarrollo es aún de vital trascendencia en nuestros días: la rueda.

La primera rueda de la que se tiene constancia fue usada en Ur (Mesopotamia) en torno al año 3500 a. C. Sin embargo, pese a que no existen evidencias arqueológicas, se cree que podría tener un

origen anterior, situado en Sumeria, en torno al año 8000 a. C. En una primera fase de desarrollo se trataría del resultado de la lenta evolución de la combinación del rodillo y de una especie de trineo. Sea como fuere, nuestros ancestros tardaron millones de años en dar ese primer paso. Muy al contrario, en la era moderna, los acontecimientos se han precipitado de forma incontenible.

Las luchas por el poder, la comida, el agua o el territorio siempre han acompañado al ser humano, originando disputas ya en la prehistoria. El campo de batalla de todos los conflictos desde la Antigüedad ha sido, por antonomasia, la tierra. Aquel que dominaba el territorio imponía su ley.

Mucho más tarde, con el desarrollo de los primeros barcos, se añadió a este campo de batalla el ámbito de las aguas. Los primeros pueblos que utilizaron el medio acuático para lograr sus objetivos por la fuerza fueron los babilonios. Los asirios ya poseían barcos de guerra en el año 3000 a. C., y sus cascos de madera eran cortos y casi redondos. Eran esencialmente naves con remos, aunque disponían de un mástil en el que izaban una vela cuadrada.

Miles de años después, otro elemento se convirtió en posible escenario de conflictos y disputas: el aire. La primera utilización del elemento aéreo con fines bélicos se remonta a noviembre de 1792. Se trataba de los primeros ensayos realizados por un grupo de artilleros en el Real Colegio de Artillería de Segovia que, dirigidos por Louis Proust, hicieron demostraciones de vuelo de un globo aerostático, cuya finalidad era obtener información relativa a las defensas de una plaza o al dispositivo de ataque a una plaza sitiada. El mundo había evolucionado: se trataba de los primeros conatos de utilización del elemento del aire como medio militar.

Estos tres elementos (tierra, mar y aire) constituían hasta entonces los tres principales campos de batalla del ser humano, por lo que fueron claves en el desarrollo del ejército moderno, con los tradicionales tres ejércitos.

La primera mitad del siglo xx nos llevó a un escenario armamentístico que pudo acabar con la extinción de la humanidad. Dos guerras mundiales, el comienzo de la era nuclear y un escenario geopolítico en el que el ser humano tenía, por vez primera, la

inquietante capacidad no sólo de autoextinguirse, sino, además, y de forma colateral, de acabar con todo atisbo de vida en el planeta.

Dentro de ese escenario de conflicto apareció un nuevo elemento: el espacio. Se trata, eso sí, de un elemento singular. Su lejanía y aparente irrelevancia en la vida diaria de las personas, unida al alto coste que supone invertir en el desarrollo espacial, hace que sólo unas pocas potencias mundiales hayan tenido interés y capacidad reales en la conquista de este elemento. Ésa es la razón por la que no todos los países cuentan con el medio espacial como ámbito de sus fuerzas militares básicas.

Tierra, mar, aire, espacio…

En las últimas dos décadas, con el desarrollo de internet y la sociedad conectada, aparece un nuevo elemento, tal vez el más singular e imprevisible de todos. Se trata de una nueva dimensión virtual a la que todos estamos expuestos y que, por primera vez, cambia los equilibrios tradicionales, convirtiendo a todos los individuos —a todos nosotros— en piezas del tablero de la sociedad conectada.

Además, toda la evolución descrita con anterioridad ha igualado los roles entre los países, de tal forma que las grandes potencias, que merced a su supremacía en los cuatro elementos o medios conocidos (tierra, mar, aire y espacio) parecían invulnerables, pasan a estar gravemente expuestas a la acción de países, organizaciones e individuos particulares que hasta el momento no representaban ninguna amenaza real.

El que domina la información y la sociedad conectada controla el mundo. Países enteros, gobiernos, ejércitos, terroristas, anarquistas y los activistas del mundo *underground* son conscientes de esto, y están actuando, sin que lo sepas, con ese fin en el ciberespacio.

Aquí comienza nuestra historia, cuya realidad es casi desconocida y supera con creces la ficción.

Internet se ha convertido ya en el «quinto elemento».

1

# ¿Cómo hemos llegado aquí? Un viaje por el tiempo

Te propongo un juego: un acertijo. ¿Qué tienen en común Muhammad Alí, Jane Fonda, Martin Luther King, Ban Ki-moon, Angela Merkel, el papa y tú mismo? Es posible que tengas el golpe de derecha de Cassius Clay, las dotes interpretativas de Fonda, la ensoñada oratoria de King, la medida diplomacia del secretario general de la Organización de las Naciones Unidas (ONU), el firme estatismo de la canciller de Alemania y el fervor religioso del papa Francisco cuando el San Lorenzo salta a la cancha. Aunque lamento confirmarte que nada de lo anterior es lo que os une. Ah, se me olvidaba decirte que te he hecho trampas: éste no es un juego cualquiera, es real.

Ese vínculo entre vosotros del que te hablo existe, y voy a demostrártelo. Ten un poco de paciencia, subamos al DeLorean y viajemos al pasado: lo mejor será que empecemos por el principio.

## Los papeles del Pentágono

Estamos en 1967. San Francisco vive su «verano del amor». La ciudad se ha inundado de jóvenes que lucen flores en el pelo y le cantan a la paz y a la liberación sexual. El movimiento *hippie*, el feminismo y el ecologismo viven su clímax, y en el viento flotan las respuestas con esencia de hierba de una nueva generación.

A esa misma hora, y a miles de kilómetros de allí, en Washington, un hombre camina en círculos sobre la densa alfombra que cubre su despacho. Nervioso y taciturno, dos sombras violáceas bajo sus ojos delatan sus habituales desencuentros con la almohada. Cuenta por toda compañía con un vaso de whisky sin hielo y un cigarrillo perenne que sostiene con dedos temblorosos. Todavía no sabe que será esa misma compañía la que acabará con su vida no demasiado tiempo después. Es Lyndon B. Johnson.

El presidente ha pedido que no le pasen llamadas. Qué lejos quedan los días felices de su gran victoria electoral, cuando arrasó a los republicanos con más del 61 por ciento de los votos. Y de eso sólo hace tres años. Pero la guerra en Vietnam ha convertido su sueño presidencial en una pesadilla que está a punto de hacerle renunciar a la reelección. El número de bajas en el ejército de Estados Unidos se ha disparado. Los norteamericanos están sucumbiendo a la guerra de guerrillas que les han planteado los norvietnamitas y al desgaste de librar batallas en la jungla. La opinión pública no quiere ver llegar más ataúdes con muchachos que deberían estar jugando en los billares o estudiando para sus exámenes de la universidad. Las manifestaciones pacifistas se suceden de costa a costa por todo el país, y la popularidad de Johnson se ha desplomado.

Por si fuera poco, está lo de ese boxeador rebelde, Muhammad Alí, antes llamado Cassius Clay. Alí ha sido llamado a filas para combatir en Vietnam, pero el muy testarudo ha declarado: «Tío, no tengo nada contra esos vietcong», y se ha negado a viajar. Como castigo, ha sido condenado a cinco años de prisión y se le ha desposeído de su título de campeón del mundo de los pesos pesados, siéndole también retirada su licencia para competir.

Desafortunadamente para Johnson, estas medidas no han tenido el efecto deseado. El caso de Alí ha despertado una enorme corriente de simpatía ciudadana hacia la figura del boxeador, que parece más decidido que nunca a pelear fuera del *ring* contra la guerra.

También Martin Luther King se ha convertido en un quebradero de cabeza para las autoridades. Su activismo en defensa de los derechos civiles, y de los afroamericanos particularmente, está generando disputas sociales, y ahora también se ha sumado a las protestas pacifistas pronunciando un elocuente discurso en el que habla de «romper el silencio» contra la guerra de Vietnam.

Poco después, una joven Jane Fonda, que ya es estrella de cine, viajará a Vietnam para inmortalizarse junto a combatientes norvietnamitas, subiendo varios grados la temperatura del conflicto.

El Gobierno estadounidense trata de mantener una imagen pública de optimismo respecto a tal ofensiva, pero los medios de comunicación han lanzado una gran campaña antibélica, encabezada por periodistas como Tom Wicker, célebre columnista de *The New York Times*, o Art Buchwald, el escritor humorístico de *The Washington Post* que años después ganará el Pulitzer.

Y, si el optimismo de Johnson en privado hace tiempo que se evaporó, su optimismo público también tiene los días contados. En este momento, un joven y prometedor economista de nombre Daniel Ellsberg acaba de regresar de servir en Vietnam. A pesar de su juventud, tiene una amplia experiencia en inteligencia militar. Antes de combatir en la guerra ha trabajado como analista estratégico en la Corporación RAND, una especie de *think tank* (o instituto de investigación) que forma a los miembros de las fuerzas armadas de Estados Unidos. También ha servido en el Pentágono bajo la tutela del secretario de Defensa, Robert McNamara.

Terminada su estancia en Vietnam, ha reingresado en la Corporación RAND, de nuevo a las órdenes de McNamara, que le ha hecho un encargo muy especial. Ellsberg forma parte de un estudio de alto secreto sobre los documentos clasificados de la gestión de la guerra, y es una de las pocas personas que tiene acceso a la totalidad de los archivos gracias a un permiso de seguridad de alto

nivel. Muy pronto, estos documentos serán mundialmente conocidos como los «papeles del Pentágono».

Ellsberg es un buen soldado, un teniente primero leal y un brillante intelectual, pero el curso de la ofensiva en Vietnam está a punto de colisionar con la línea de flotación de sus valores. En poco tiempo comenzará a asistir a actos y conferencias contra la guerra, lo cual le hará tomar conciencia de lo que está sucediendo en Vietnam y de cómo el Gobierno de su país lleva años engañando a los ciudadanos y al Congreso sobre un asunto de importancia estratégica.

Dentro de tres años, y ayudado por un excompañero de la Corporación RAND y de miembros del equipo del senador Edward Kennedy, Ellsberg realizará en secreto varios juegos de fotocopias de los documentos clasificados en los que está trabajando. Los papeles del Pentágono revelarán que Jonhson tenía conocimiento desde el principio de que la guerra difícilmente podía ser ganada, y de que su prolongación produciría un número muy elevado de bajas, algo nunca reconocido públicamente.

Ellsberg entregará las pruebas al diario *The New York Times*, pero la administración del ya presidente Nixon solicitará una orden judicial para paralizar la publicación. Será la primera vez que un Gobierno federal es capaz de detener una edición desde los tiempos de Abraham Lincoln, durante la guerra de Secesión. Daniel distribuirá entonces los documentos a *The Washington Post* y a otros 17 periódicos, y, poco después, el Tribunal Supremo autorizará al *Times* a reanudar la publicación, en una sentencia histórica que será considerada como uno de los pilares modernos de la libertad de prensa recogida en la Primera Enmienda.

La filtración de los papeles del Pentágono desatará una campaña de desprestigio contra Ellsberg, orquestada por Nixon y Kissinger. Los agentes del FBI y de la CIA George Gordon Liddy y Howard Hunt (dúo que será conocido como «los fontaneros») pincharán el teléfono de Ellsberg e irrumpirán en la oficina de su psiquiatra, el doctor Lewis Fielding, en busca de materiales con los que chantajear a Ellsberg. Este mismo tipo de «trucos sucios» de sus «fontaneros»

son los que provocarán la caída final de Nixon tras el caso Watergate.

Nixon y Kissinger buscarán la condena de Ellsberg por robo, conspiración y espionaje, pero su caso será desestimado cuando aparezcan evidencias sobre las escuchas telefónicas ilegales y el allanamiento ordenados por el Gobierno. Después, Ellsberg escribirá varios libros, continuará siendo un activo promotor de la paz y será galardonado con diversos premios en reconocimiento a su contribución a un mundo más seguro y transparente.

En 1967, Daniel Ellsberg todavía no se ha convertido en el mayor soplón de la historia de Estados Unidos hasta ese momento. Sin embargo, son tantos los frentes abiertos contra la guerra de Vietnam que Johnson empieza a temer que el movimiento pacifista pueda contar con algún tipo de financiación o ayuda exterior. Así, después de varias conversaciones con la Agencia Central de Inteligencia (CIA) y la Oficina Federal de Investigación (FBI), el presidente apura el enésimo cigarrillo del día y levanta el teléfono: esto es un caso para la NSA.

NSA son las siglas en inglés de la Agencia de Seguridad Nacional de Estados Unidos, aunque también circula un atinado chiste que asegura que se trata de la forma abreviada de *No Such Agency* («no existe tal agencia»). Y digo atinado porque, durante años, la NSA oficialmente no existía. Fue fundada en secreto en 1952 por el entonces presidente Harry S. Truman, para dar alertas tempranas ante potenciales ataques como el de Pearl Harbor. Sin embargo, a lo largo de dos décadas operó siempre en la sombra, y su existencia no fue reconocida sino hasta los años setenta. Hoy en día la NSA es el enemigo público número uno de la libertad en internet. Los ojos del Gran Hermano.

Puede afirmarse, por tanto, que cuando Lyndon B. Johnson levanta el teléfono aquella tarde de 1967 lo hace para marcar el número de un fantasma. Sorprendentemente, al otro lado del aparato responde en seguida una voz que suena cercana y familiar —nunca comunicarse con un espectro resultó tan fácil—: es el director de la NSA, que depende del Departamento de Defensa.

La misión de la agencia, tal como aparece señalado hoy en su página web, consiste en «prevenir que adversarios extranjeros accedan a información sensible o clasificada vinculada con la seguridad nacional», además de «recolectar, procesar y diseminar información de inteligencia de fuentes externas para propósitos de inteligencia y contrainteligencia, y para respaldar operaciones militares». Y lo que teme Johnson es precisamente que algún rival extranjero esté intentando dañar la seguridad nacional suministrando apoyo a los grupos de oposición a la guerra de Vietnam.

La conversación dura pocos minutos, y su resultado, hoy desclasificado, es la creación de un nuevo proyecto de seguridad, el proyecto Minarete. A continuación, la NSA iniciará un gran despliegue para espiar las llamadas telefónicas, así como los mensajes de cable y télex de algunos de los líderes del movimiento antibélico. El seguimiento se prolongará durante seis años, hasta 1973, continuando tras el relevo presidencial de Johnson, al que Nixon sucederá en el cargo.

La lista de vigilancia de personalidades contiene más de 1.600 nombres, y entre los elegidos están el boxeador Muhammad Alí, los activistas Whitney Young y Martin Luther King, la actriz Jane Fonda, el senador demócrata Frank Church, el republicano Howard Baker y los periodistas Tom Wicker y Art Buchwald.

Me dirás que vuelvo a hacer trampas, que esto sólo explica qué tienen en común Muhammad Alí, Martin Luther King y Jane Fonda, pero que no da cuenta de su vínculo con Ban Ki-moon, Angela Merkel ni el papa Francisco. Y, sobre todo, me dirás que no explica nada de qué rayos tienes tú que ver con toda esta gente. Ten un poco más de paciencia, te lo contaré todo. En los próximos minutos. Subamos de nuevo al DeLorean.

## Wikileaks

Hemos dado un salto de más de cuarenta años. Ahora estamos en 2010. Un chico de veintidós años de edad chatea en su ordenador portátil. Tiene la tez pálida y los ojos pequeños y azules; su pelo rubio luce cortado al rape. Se llama Brad, y su vida no es sencilla. A pesar de su aspecto frágil y su corta edad, el muchacho es un soldado de primera clase de Estados Unidos. Su condición de homosexual le ha puesto las cosas difíciles en su trabajo, pues todavía no se ha derogado la ley que prohíbe a los homosexuales servir abiertamente en las fuerzas armadas estadounidenses, motivo por el que es probable que le despidan. Además, Brad no encaja bien con el resto de sus compañeros; algunos de ellos, incluso, le han retirado la palabra por el simple hecho de ser gay. El joven no es feliz, y lleva un tiempo sospechando que sus problemas psicológicos pueden estar relacionados con un trastorno de identidad de género: Brad quiere ser una mujer.

Así lo explica él mismo mientras chatea en su ordenador: «Soy un analista de inteligencia del ejército, estoy destinado en el este de Bagdad y permanezco a la espera de ser licenciado por "problemas de adaptación", en lugar de por un trastorno de identidad de género».

Como ves, las cosas no le van muy bien en el trabajo. Ya ha sido reprendido en varias ocasiones por divulgar más información de la debida en los mensajes de vídeo que envía a su familia y a sus amigos, y que cuelga en Youtube. De hecho, han estado a punto de descartarle para la misión a Irak porque sus superiores le consideran «un peligro para sí mismo y, posiblemente, para otros»; pero, finalmente, la acuciante necesidad de tener suficientes trabajadores del servicio de inteligencia sobre el terreno ha determinado que fuera enviado a la zona de guerra.

Su trabajo consiste fundamentalmente en asegurarse de que los otros analistas de inteligencia del grupo disponen de acceso a todo aquello que están autorizados a ver. Esta posición le ha abierto la puerta a una ingente cantidad de datos alojados en la red de ordenadores del Gobierno estadounidense.

Brad continúa chateando, oculto tras el *nickname* de *dawgnetwork*. Cada día se siente peor. Sus problemas personales, unidos a la consternación que le provoca la guerra, le han hecho tomar una decisión. No hay vuelta atrás. «La información debe ser libre», escribe. Al otro lado de la pantalla de su ordenador, quien lee y teclea es Julian Assange.

Assange es el director de Wikileaks, proyecto al que lleva vinculado desde el año 2006, cuando terminó sus estudios de física y matemáticas en la Universidad de Melbourne. Desde muy joven ha sido un apasionado de la informática, destacando como precoz hacker y programador; y Wikileaks es la plataforma idónea para desarrollar sus proyectos. Se trata de una organización internacional sin ánimo de lucro y que, a través de su sitio web, publica informes anónimos y documentos filtrados de interés público, preservando el anonimato de sus fuentes. A principios de 2010, esta organización todavía no es muy conocida, como tampoco lo es Julian Assange. Sin embargo, eso está a punto de cambiar para siempre.

Mientras chatea con Brad, Assange comprende la magnitud de la información que tienen entre manos. La filtración de esos documentos no sólo será un bombazo mediático, sino que puede alterar el curso de las relaciones internacionales de un modo dramático. Además, la revelación le convertirá muy pronto en la persona más importante del momento.

Brad le cuenta que lleva meses recopilando información muy sensible sobre la marcha de la guerra, así como sobre las operaciones de la diplomacia de Estados Unidos en todo el mundo. El Departamento de Defensa ha prohibido en sus instalaciones los dispositivos de almacenamiento USB por temor al *malware*, en un intento por asegurar las comunicaciones del país. Sin embargo, las unidades para CD grabables siguen operativas. Brad se jacta del modo en que se ha hecho con toda esa información: «He escuchado y cantado a Lady Gaga mientras extraía la que es posiblemente la mayor fuga de datos de la historia de América».

Brad acaba de superar a Daniel Ellsberg como el mayor soplón de la historia y, de la mano de Assange, comienza a preparar su primer *boom* informativo. Se trata de un vídeo que han titulado de forma

provocadora *Asesinato colateral*, en el que puede verse un helicóptero Apache del ejército de Estados Unidos disparando sobre civiles en Irak, entre los que se encuentran dos empleados de la agencia Reuters, los cuales pierden la vida.

Para la edición del vídeo, Assange ha alquilado una casa en Islandia durante el mes de marzo de 2010; allí, él y otros activistas trabajan preparando su lanzamiento. *Asesinato colateral* verá finalmente la luz en abril. Brad quiere refugiarse en el anonimato, tal como le ha prometido Wikileaks, pero las ambiciones del hacker australiano son otras; finalmente, Assange lanza una campaña en la que trata de obtener la máxima publicidad posible, presentando el vídeo ante los medios de comunicación en el National Press Club, en Washington. Un mes más tarde, en mayo de 2010, el director de Wikileaks viaja a Australia, donde empiezan sus primeros problemas con la justicia. La policía le retira el pasaporte, que más tarde le es devuelto con la advertencia de que va a ser cancelado.

En realidad, eso no es nada comparado con lo que le espera a Brad. El muchacho ha estado chateando con otros hackers en internet y ha cometido más indiscreciones de las que debería. Desesperado por su situación personal y laboral, así como por el aislamiento total en el que está sumido, necesita encontrar a alguien en quien poder confiar, alguien que le dé el apoyo psicológico y la comprensión que necesita. Ha conocido a Adrian Lamo, un tipo bastante conocido en la escena hacker, y, sin pensárselo mucho, le ha contado todos sus secretos, incluida la filtración masiva de documentos a Wikileaks. Y lo que es más grave, le ha revelado su nombre real: Bradley Manning.

El ingenuo de Brad le cuenta: «Era información muy sensible. Y, bueno, se la mandé a Wikileaks. Dios sabe lo que sucederá a partir de ahora. Espero que haya un gran debate mundial, polémicas, reformas... Si no es así, estamos condenados como especie». Lamo le dice: «Puedes considerar esto una confesión o una entrevista que nunca será publicada, y que te permitirá contar con cierto grado de protección legal».

Lo que el soldado no sabe es que Lamo está a punto de romper su palabra y traicionar toda la confianza que Brad ha depositado en

él delatándole a las autoridades. Bradley Manning es inmediatamente detenido en Bagdad y encarcelado, sin juicio previo, en una prisión de máxima seguridad. Después, un tribunal militar lo condenará a 35 años de prisión y la expulsión con deshonor del ejército por varios delitos de espionaje y robo de secretos. Brad todavía puede sentirse afortunado: si el juez lo hubiera encontrado también culpable de colaborar con el enemigo, le habría caído cadena perpetua.

Para empezar, Brad es confinado durante nueve meses en una prisión de Quantico (Virginia), donde se le aplican unas condiciones de reclusión terribles que le obligan a permanecer veintitrés horas al día encerrado en su celda, sin almohada, sin sábanas ni objetos personales y despojado de las gafas que debe llevar por prescripción médica. El único ejercicio que se le permite hacer es caminar por una habitación vacía, y para dormir es obligado a desnudarse, a excepción de la ropa interior.

Sus condiciones de encarcelamiento mejoran tras el traslado a la prisión militar de Fort Leavenworth, en el estado de Kansas; pero Manning deberá pasar entre rejas los siguientes 35 años, que son muchos más de los que tenía entonces. Brad no es el mismo hombre que antes de Wikileaks, de hecho, ya ni siquiera es un hombre. En 2014, por fin consiguió que el mismo ejército estadounidense aprobara su operación para cambiar de sexo y convertirse en mujer. Ahora tiene una nueva identidad, para la que ha elegido el nombre de Chelsea, Chelsea Manning.

El tratamiento y juicio de Manning por parte de las autoridades de Estados Unidos ha sido objeto de numerosas críticas en todo el mundo. Desde amplios sectores de la sociedad civil y desde numerosas organizaciones no gubernamentales (ONG) se ha cuestionado la imparcialidad de la justicia. Son muchos los que creen que Chelsea Manning debería ser considerada una heroína de los derechos humanos, y no una criminal. La propia Amnistía Internacional declaró antes del juicio que «consideraría motivo de preocupación que un Gobierno intentara castigar a una persona que, por razones de conciencia y de manera responsable, hubiera

publicado información con el convencimiento razonable de que esa información era prueba de violaciones de derechos humanos».

Sin embargo, ninguna protesta podrá cambiar el destino de Chelsea Manning, como no ha podido cambiarlo la defensa de su abogado, que apeló a la frágil salud mental de su cliente y a sus buenas intenciones durante el juicio, y que ha solicitado a Obama el indulto, aunque sin éxito. Chelsea parece resignada a su suerte: «Si rechaza mi perdón cumpliré mi tiempo sabiendo que, a veces, hay que pagar un alto precio para vivir en una sociedad libre», le ha dicho al presidente.

Mientras tanto, las cosas también empiezan a ponerse negras para Assange, que dice sentirse perseguido por el Gobierno estadounidense. No obstante, ni eso ni el precedente de Manning parecen poder poner freno a su determinación de hacer públicas las filtraciones de Chelsea. En julio y octubre de 2010 da a conocer un gran tesoro informativo en forma de documentos clasificados relacionados con las guerras de Afganistán e Irak. El director de Wikileaks ha trabajado con *The New York Times*, *The Guardian* y *Der Spiegel* para verificar, analizar y presentar dichos documentos. Por supuesto, no han gustado nada a las autoridades norteamericanas, que han condenado la publicación en términos muy duros y han ordenado la persecución de las fuentes responsables de la filtración.

Pero nada detiene a Assange y, pocos meses después, Wikileaks lanza una nueva bomba virtual, que esta vez lleva el nombre de «Cablegate». Se trata de más de 250.000 cables, o mensajes confidenciales, del Departamento de Estado, escritos por 271 embajadas y consulados estadounidenses en 180 países. Los documentos abarcan desde 1966 hasta febrero de 2010, y contienen un buen número de secretos embarazosos que ponen en evidencia que Estados Unidos ha estado utilizando a sus diplomáticos para espiar a sus aliados, incluyendo al secretario general de la ONU Ban Ki-moon.

Los cables mencionados detallan lo que el Departamento de Estado denomina *human intelligence* (inteligencia humana), que hace referencia a la información conseguida a través de contactos personales o mediante la relación informal. Aunque sin la expresa

intervención de los servicios secretos, el espionaje encomendado a los funcionarios de embajadas y misiones abarca cientos de asuntos de interés estratégico para Estados Unidos: desde las gestiones y la apariencia física de los diplomáticos iraníes y norcoreanos en Nueva York hasta las negociaciones de paz en Palestina, pasando por los planes e intenciones del secretario general de la ONU y su equipo, las relaciones de Hamás y Hizbulá, las armas nucleares o los choques militares, étnicos y guerrilleros africanos.

Assange llega a un acuerdo con algunos de los diarios más prestigiosos del mundo para la publicación de los documentos. *The New York Times*, *The Guardian*, *Le Monde*, *Der Spiegel* y *El País* se comprometen a difundir únicamente aquellos cables «sujetos a una edición conjunta e integral y a un proceso de autorización». Publicarán toda la información que estimen relevante, pero editarán el contenido que pueda poner en peligro a las personas citadas en los cables o a los informantes secretos.

Sin embargo, poco después ocurre un error fatal. La clave de acceso al total de los documentos es revelada «accidentalmente», tras un malentendido por el que se culpan mutuamente *The Guardian* y Julian Assange. El director de la organización acusa al diario de haberla desvelado en un libro titulado *Wikileaks y Assange*, publicado por dos de sus periodistas, David Leigh y Luke Harding. Por su parte, *The Guardian* rechaza cualquier tipo de responsabilidad en relación con la publicación de los cables íntegros. David Leigh sostiene que el propio Assange le aseguró que la clave que le proporcionó funcionaría sólo durante un breve periodo de tiempo y que, por lo tanto, ya no sería válida una vez publicado el libro.

Sea como fuere, una vez que el acceso a la información ha sido facilitado, Wikileaks cree que ya no hay motivo para no publicar el nombre de las fuentes, y decide hacer públicos en su web todos los documentos sin editar.

A los pocos días, Assange revelará decenas de miles de cables diplomáticos en los que, por primera vez, la organización no oculta el nombre de los informantes. Los nuevos archivos identifican a personas que figuran bajo el epígrafe de «estrictamente protegidos», la fórmula que Washington utiliza para referirse a

aquellos documentos cuya publicación podría poner en riesgo a los sujetos mencionados. En los cables aparecen también los nombres de activistas y de individuos perseguidos por sus gobiernos. Esta decisión desata la ira de Estados Unidos y Australia, que denuncian que la actitud irresponsable de los activistas puede poner en peligro la seguridad de las fuentes citadas.

La medida también cae como un jarro de agua fría para *The New York Times*, *The Guardian*, *Le Monde*, *Der Spiegel* y *El País*, que emiten un comunicado conjunto en el que reprueban la decisión de Wikileaks: «Continuaremos defendiendo nuestros proyectos de colaboración anteriores. No podemos, sin embargo, defender la publicación innecesaria de la base de datos al completo. Es más, la condenamos conjuntamente». Y añaden: «La decisión de publicarlos le corresponde única y exclusivamente a Julian Assange. Él debe responsabilizarse de esa decisión».

El semanario alemán *Der Spiegel* abundará en las críticas anteriores, advirtiendo a la organización de que la «cadena de errores, descuidos, indiscreciones y confusiones» que ha hecho posible la filtración de la información tendrá consecuencias sobre la credibilidad de la página, y de que podría disuadir a potenciales «gargantas profundas» de ofrecer documentos a Wikileaks.

Además, Reporteros sin Fronteras ha decidido dejar de respaldar a la organización, anunciando que cancelará de forma temporal la página web con la que aseguraba la supervivencia del contenido de Wikileaks en caso de que la web de filtraciones sufriera un ciberataque: «Por un lado, algunos de los nuevos cables no han sido editados y muestran los nombres de informantes de varios países, incluidos Israel, Jordania, Irán y Afganistán. A pesar de que no se ha podido demostrar que hasta el momento se haya puesto en peligro ninguna vida, las consecuencias que podría tener para los informantes —represalias laborales, ataques físicos y otras— no pueden ser ignoradas», asegura en un comunicado. Además, Reporteros sin Fronteras ha acusado a Wikileaks de haber dado a los gobiernos democráticos «buenas razones para poner internet bajo estrecha vigilancia», a lo que la web de filtraciones ha respondido con sorna: «*Reporteros Sin Verificar los Hechos* ha emitido un

comunicado idiota, basado en un montón de citas que jamás hemos hecho».

Lo cierto es que, aunque intenten tomárselo con humor, las cosas empiezan a ponerse feas para Julian Assange y Wikileaks. Las acusaciones de haber puesto en riesgo la vida de personas se han convertido en una amenaza real, y no sólo para funcionarios de la administración norteamericana. En China, por ejemplo, grupos nacionalistas desataron una caza de brujas para perseguir a los disidentes que aparecen identificados en los cables. En Estados Unidos, el director nacional de inteligencia ya considera que el caso Cablegate tendrá un impacto notable sobre la seguridad nacional, y son muchos los que piden que Assange sea juzgado por espionaje.

Comienza a estrecharse el círculo sobre el hacker australiano. El banco suizo en el que tiene alojada una cuenta decide cerrársela, alegando irregularidades de procedimiento: al parecer, Assange había afirmado tener su residencia en Ginebra cuando abrió el depósito, lo cual se reveló falso posteriormente.

Y esto no ha hecho más que empezar. La fiscalía sueca dicta una orden de busca contra Assange, al que acusa de cometer un delito de violación, abusos sexuales y coacción. Después de combatir sin éxito la orden de extradición, el líder de Wikileaks pide asilo a la embajada de Ecuador en Londres, y cede la dirección de la organización a Kristinn Hrafnsson.

Al mismo tiempo, el acoso para impedir la financiación de la web se hace más intenso. PayPal anuncia que, en adelante, no permitirá enviar dinero a la cuenta de Wikileaks, siguiendo las directrices del Gobierno de Estados Unidos, que ha declarado ilegal la actividad de la asociación. Del mismo modo, MasterCard y Visa dificultan que los seguidores de Assange puedan contribuir económicamente al soporte técnico y legal del sitio web.

A pesar de todo ello, Wikileaks consigue mantenerse a flote. Todos los documentos continúan disponibles en internet para quien quiera consultarlos, y la web sigue manteniendo su actividad. La persecución a la que están sometidos no es óbice para que publiquen una cantidad ingente de documentos relacionados con la guerra en Siria y el espionaje al que la NSA tiene sometido al

régimen de Bashar al-Assad, incluidos dos millones de correos electrónicos del régimen alauí y la mensajería personal del dictador.

Wikileaks se ha convertido en un fenómeno mundial y en el símbolo de la libertad en internet. Su modelo ha servido de inspiración para otros grupos de activistas locales o internacionales. Su popularidad es tal que Julian Assange es elegido hombre del año 2010 por la revista *Time*.

Sin embargo, la gloria tiene un precio. Assange permanece recluido en la embajada de Ecuador en Londres, y su futuro es incierto. Y Chelsea Manning va a pasar el resto de su juventud y la mayor parte de su vida en una prisión militar.

Con la historia de Manning, Assange y Wikileaks hemos despejado otra incógnita de la ecuación que planteamos al principio de este capítulo. Ya sabemos qué tiene en común Ban Ki-moon con Muhammad Alí, Martin Luther King y Jane Fonda: todos ellos han sido sometidos a algún tipo de vigilancia por parte de los servicios de inteligencia de Estados Unidos.

Pero todavía nos queda por conocer la relación que todos ellos guardan con Angela Merkel y el papa Francisco; y, por supuesto, no hemos explicado cómo demonios puedes estar vinculado tú con este grupo tan heterogéneo de personajes públicos.

Nos vamos aproximando al final de la historia, pero todavía hemos de viajar un poco más en el tiempo antes de poder regresar al presente. Sube al DeLorean y abróchate el cinturón, que vienen curvas.

## El caso Snowden

Ahora estamos en junio de 2013. En una pequeña habitación de un hotel de Hong Kong, un hombre de veintinueve años de edad mira el reloj por encima de sus gafas. Se llama Edward y parece inquieto. A decir verdad, es normal que lo esté: lleva meses esperando la reunión que tendrá lugar dentro de unos minutos.

Edward acaba de llegar a la antigua colonia británica procedente de Hawái, donde hasta hace muy poco trabajaba como administrador de sistemas para el contratista de defensa Booz Allen Hamilton, dentro de la NSA. Se ha ausentado solicitando una excedencia temporal para someterse a un tratamiento contra la epilepsia que padece, pero no tiene ninguna intención de reincorporarse a su puesto. También ha trabajado para la NSA en Japón y, antes de eso, ha sido empleado de la CIA en Ginebra, donde desempeñaba el cargo de experto en seguridad informática.

En Hawái, Edward ha tenido una vida apacible junto a su novia, y ha disfrutado de un sueldo de 200.000 dólares que le ha permitido vivir muy desahogadamente. Sin embargo, toda esa tranquilidad ya es historia. Y lo más sorprendente de todo es que ha renunciado a esa tranquilidad por voluntad propia.

Las personas a las que Edward espera en su hotel de Hong Kong son Laura Poitras, Ewen MacAskill y Glenn Greenwald. Poitras es una reconocida realizadora de documentales especializada en vigilancia, MacAskill es un periodista del diario británico *The Guardian* y Greenwald es un abogado y bloguero que cuenta con una columna en ese mismo periódico, una columna desde la que ha emprendido una auténtica cruzada contra la vigilancia de los gobiernos.

Edward contactó por primera vez con Greenwald en diciembre de 2012, pero el abogado no disponía de un programa PGP (Pretty Good Privacy) que le permitiera encriptar las comunicaciones, y tampoco pensaba tomarse la molestia de conseguir uno para hablar con un tipo que no se había identificado y no le ofrecía más que una insinuación vaga.

Sin embargo, Edward no se da por vencido, y decide escribir a Laura Poitras, a la que ha descubierto al leer una de las columnas de

Greenwald. Poitras se encuentra en su apartamento de Berlín cuando recibe el misterioso correo de alguien que se hace llamar Citizenfour. A diferencia de Greenwald, ella sí dispone de un programa de encriptación, pero el remitente la instruye sobre cómo utilizar un canal de comunicación todavía más seguro. Después, Edward se presenta como un «miembro de alto nivel de la comunidad de inteligencia» y le asegura a la cineasta que hablar con él «no será una pérdida de tiempo».

Edward también mantendrá contacto con Bart Gellman, un periodista de *The Washington Post* al que hará cuantiosas revelaciones sobre los programas de espionaje masivo de la NSA, pero la relación con su confidente se enfriará después de solicitarle que publique unos documentos en el *Post* en menos de 72 horas, algo que Gellman ni puede ni quiere hacer.

Tras meses de intercambios de información confidencial con Gellman, Poitras y Greenwald, a quien la realizadora ha incorporado al equipo, Edward decide que ha llegado el momento de que se conozcan en persona: deben tomar un vuelo a Hong Kong para mantener una reunión cara a cara.

Descartado Gellman para la misión, Poitras y Greenwald inician los preparativos del viaje. A pesar de que Greenwald lleva sólo unos meses trabajando para *The Guardian*, el diario lo autoriza a viajar, pero con la condición de que les acompañe un periodista veterano y que goce de la confianza de la dirección. Se une así al grupo Ewen MacAskill. Al día siguiente, los tres toman un avión con destino a Hong Kong, sumidos en la incertidumbre de no saber qué les depara el destino.

Aterrizan en la antigua colonia británica el 1 de junio para entrevistarse con Edward dos días después. El extrabajador de la CIA y la NSA les ha dado unas directrices de localización propias de una película de Hollywood; deben situarse en la entrada de cierto restaurante y esperar a que él pase; para que le reconozcan, Edward llevará un cubo de Rubik en las manos.

Poitras y Greenwald dejan a MacAskill en su hotel para no despertar recelos en su fuente, que no le conoce, y se presentan a la hora acordada en el lugar establecido. En seguida aparece un

muchacho de aspecto muy joven llevando un cubo de colores. Greenwald le pregunta: «¿A qué hora abre el restaurante?», a lo que Edward responde: «A mediodía. Pero no vayan ahí, la comida es malísima». Y añade: «Síganme».

En silencio, los dos periodistas siguen a su informante hasta un hotel, toman el ascensor hasta la décima planta y se internan en una habitación, la 1.014. Una vez allí, Edward se presenta: «Me llamo Edward Joseph Snowden». Greenwald repara en un vaso lleno de agua que descansa, de forma aparentemente incomprensible, junto a la puerta, y en una servilleta desplegada al lado del vaso que luce una mancha oscura. Al parecer es un viejo truco de espías para saber si alguien ha entrado en tu habitación en tu ausencia. De ser así, el agua del vaso se habría derramado al abrir la puerta sobre la servilleta impregnada de salsa de soja, cambiando el aspecto de su mancha y delatando la intrusión.

Casi de inmediato, los tres se ponen a trabajar. Al principio, Snowden se muestra tímido y nervioso, pero convencido de que está haciendo lo correcto por el «interés público» y mentalizado de que la decisión que ha tomado le va a cambiar la vida: reconoce sin ambages que ni su familia ni su novia saben que ha huido y que es posible que pase mucho tiempo antes de que pueda volver a verlos. Poitras inicia la filmación de la reunión a los pocos minutos, mientras Greenwald y Snowden comienzan a hablar sobre los documentos y sobre cómo ordenarlos para publicarlos en la prensa lo antes posible. Al día siguiente se incorpora también a las sesiones MacAskill, que al principio desconfía de Edward: parece imposible que un chico tan joven haya tenido tiempo de memorizar tal cantidad de información.

Los responsables de *The Guardian* se ponen en contacto con la Casa Blanca para hacerles saber que han recibido una filtración relativa a las actividades de espionaje llevadas a cabo por la administración estadounidense, y que tienen intención de hacerla pública de forma inminente. Sus interlocutores en la Casa Blanca, atónitos, intentan disuadir al diario de sus intenciones, pero *The Guardian* asegura que sólo se abstendrá de divulgar la información si se demuestra que su difusión pondría en peligro la vida de personas.

El Gobierno responde: «Entenderán que nosotros estamos más capacitados que ustedes para decir lo que supone un riesgo para la seguridad nacional. Ninguna empresa de comunicación seria haría eso». A lo que la directora del diario, Janine Gibson, contesta: «Entenderán que nosotros estamos más capacitados que ustedes para decir lo que es noticia».

La primera revelación verá la luz el día 6 de junio de forma simultánea en *The Washington Post* y *The Guardian*. Ambos diarios darán a conocer que la NSA, a través de un programa llamado Prism, tiene acceso a los servidores de los gigantes de internet como Google, Facebook o Apple, así como a los datos personales de cientos de millones de usuarios. Prism es el programa de vigilancia más importante que se ha descubierto desde que se hiciera público Echelon, una red de análisis de inteligencia desarrollada durante la guerra fría para interceptar las comunicaciones militares y diplomáticas, pero también privadas y comerciales.

La noticia cae como una bomba. En los días sucesivos, el equipo desplazado a Hong Kong continúa entrevistándose con Snowden y publicando nuevos datos. Será así como descubran la existencia de otros programas de vigilancia, como Tempora y XKeyscore. El programa Tempora permite a los países que forman la alianza Five Eyes (Estados Unidos, Reino Unido, Australia, Nueva Zelanda y Canadá) pinchar más de doscientos cables de fibra óptica, muchos de ellos interoceánicos, a través de los cuales se transmite la información en todo el mundo. Por su parte, XKeyscore sirve para filtrar información de correos electrónicos y redes sociales, entre otro tipo de comunicaciones, en bases de datos. Los documentos de Snowden demuestran que Estados Unidos puede rastrear los datos de los internautas sin necesidad de autorización judicial, y simplemente ingresando el nombre de usuario, la empresa proveedora del dominio y el rango de fechas a buscar. Además, las filtraciones revelan que la NSA almacena cada día 5.000 millones de datos de localización de usuarios, obtenidos a través de teléfonos inteligentes y empresas de telefonía móvil.

Pero hay más: los archivos filtrados por Snowden dan cuenta de que la NSA ha espiado el correo electrónico y los teléfonos de 35

dirigentes políticos extranjeros, entre ellos, la canciller alemana, Angela Merkel, la presidenta de Brasil, Dilma Rousseff, el papa Francisco, el mandatario mexicano, Enrique Peña Nieto, y diversos miembros del Gobierno de España, además de algunas grandes empresas, como la brasileña Petrobras.

Según los datos facilitados por Edward, Estados Unidos comenzó a espiar el teléfono de Merkel en 2002, tres años antes de que la actual canciller accediera a la jefatura del Gobierno. Obama ha negado tener conocimiento de estos hechos, pero, según los documentos de Snowden, el presidente estadounidense estaba al corriente de la situación y la había autorizado: por lo visto no se fiaba de Merkel, y quería conocer de primera mano quién era realmente esta política.

En este mismo contexto de espionaje a líderes mundiales, la NSA ordenó intervenir las comunicaciones del Vaticano, incluyendo las llamadas realizadas por Jorge Bergoglio justo antes del cónclave en el que resultaría elegido papa.

A pesar del indiscutible éxito que han tenido las filtraciones, Edward está cada vez más irritable y paranoico, sabe que la NSA lo está buscando, y que, haciendo uso de su tarjeta de crédito, es sólo cuestión de poco tiempo que lo encuentre. Ataviado con una camiseta y sentado en la cama, se tapa la cabeza con una manta mientras escribe en el portátil para evitar la activación remota de la cámara frontal del ordenador.

Decide entonces que ha llegado el momento de desvelar su identidad y comenzar a planear un plan de huida: «No me quiero esconder, quiero salir y decir que no tengo miedo», asegura. Junto con Greenwald y Poitras, graba una entrevista que se hace viral en cuestión de minutos. Pero, casualmente, un periodista identifica el hotel donde ha sido grabado el vídeo al reconocer una de las lámparas que aparecen en la grabación, lo cual precipita la huida de Snowden.

El antiguo analista de seguridad de la NSA abandona su hotel y se refugia en algún lugar de Hong Kong. En los días siguientes concederá una entrevista a un medio local en la que asegurará que Estados Unidos hackea los ordenadores de China. Las autoridades

del país asiático desconfían de Snowden, que comienza a confirmar sus sospechas de que Hong Kong ya no es un lugar seguro para él. Decide entonces seguir las recomendaciones de Julian Assange y buscar asilo en Ecuador. El 22 de junio de 2013 tomará un vuelo a Moscú, donde tiene pensado hacer escala para viajar a continuación a La Habana y llegar a Quito dos días más tarde de su partida. Sin embargo, Edward nunca alcanzará su destino.

Horas antes de iniciar su viaje, Estados Unidos le acusa de espionaje, emite una orden internacional de extradición y le cancela el pasaporte. Assange, por su parte, ha enviado a Hong Kong a la colaboradora de Wikileaks Sarah Harrison (de quien se dice que es su novia) para asesorar legalmente a Snowden. Tras hacer algunas averiguaciones, ambos llegan a la conclusión de que el Gobierno chino no le pondrá demasiadas trabas para abandonar el país: al parecer quieren lavarse las manos en todo este asunto.

Así, nervioso pero decidido, Edward se presenta con Sarah en el aeropuerto para tomar su avión a Moscú. Mientras caminan por la terminal son conscientes de que les siguen agentes chinos de paisano. Sin embargo, ninguno se acerca a ellos ni hace intención de impedir su viaje. Snowden presenta su pasaporte en el control de seguridad. El corazón le palpita a doscientos latidos por minuto, y un sudor frío le resbala por la frente. El funcionario que se yergue tras el mostrador lo mira durante unos instantes que a él, como prófugo, le parecen eternos, y luego le deja pasar.

Lo han conseguido, están volando a Moscú. Lo que no sospechan es que ya se agolpan, aguardando su llegada, decenas de periodistas en el aeropuerto de Sheremétievo. Un chivatazo de alguien del Gobierno chino les ha puesto sobre aviso. Los medios también saben que, en unas horas, Snowden partirá en un vuelo de enlace a La Habana desde la capital rusa. Muchos reporteros se apremian para comprar un billete en el mismo vuelo. Pero, a pesar de la expectación despertada, Edward nunca subirá a ese avión. La próxima imagen que se tendrá de él llegará meses más tarde, en octubre. Una fotografía muestra a Snowden retratado en un barco junto a Sarah Harrison, en un río de algún lugar de Rusia.

Hace menos de un año, Edward era un joven con una carrera brillante, un sueldo envidiable y una vida apacible con su novia en las islas Hawái. Hoy vive como un fugitivo, con una existencia que él mismo ha definido como la propia de un «gato casero». Apenas sí sale de su casa, y cambia de domicilio con mucha frecuencia. El contacto con su familia o con el exterior es mínimo. Es el precio que ha decidido pagar por convertirse en el mayor soplón de la historia de Estados Unidos, superando a Chelsea Manning y Daniel Ellsberg, los otros dos miembros de este podio de honor. O de deshonor. Héroes para unos, traidores para otros.

Pero ¿por qué lo hicieron? ¿Qué puede llevar a alguien a cambiar su vida y a ponerla en riesgo para el resto de sus días? En contraespionaje existe un formulario para evaluar las motivaciones psicológicas de quienes se convierten en traidores o dobles agentes. Se lo conoce con el acrónimo MICE —dinero, ideología, coacción y ego.

Para quienes lo consideran un traidor, Snowden puntúa muy alto en ego. La forma de pavonearse en sus apariciones de internet y la jactancia que exhibe en sus declaraciones (dijo que él podría espiar hasta al presidente de Estados Unidos si quisiera), llevan a algunos expertos a pensar que Edward es un narcisista.

Para otros, en cambio, la explicación a la traición de Snowden hay que buscarla en la letra «I», la de ideología. Según ellos, Snowden es un auténtico creyente de lo que hace. Tal como sostiene un antiguo oficial de inteligencia estadounidense: «Con Manning era evidente que había un trastorno psicológico y emocional detrás, pero Snowden parece movido por la convicción de que toda información debe ser libre».

Héroes o traidores, los tres protagonistas de este viaje en el tiempo, Daniel Ellsberg, Chelsea Manning y Edward Snowden, nos han permitido repasar los casos más importantes y escandalosos sobre espionaje y filtración de documentos de toda la historia. Ahora sabemos qué tienen en común Muhammad Alí, Jane Fonda, Martin Luther King, Ban Ki-moon, Angela Merkel y el papa Francisco: todos ellos han sido vigilados y espiados por los servicios de inteligencia estadounidenses.

¿Y tú? Bueno, tú no ibas a ser menos. Tú eres una de las cientos de millones de personas vigiladas por la NSA. Tienen tus correos electrónicos, tus llamadas de móvil, tus mensajes de texto, tus fotografías de Instagram, tu información de Facebook, tu ubicación en Google Maps. Saben las páginas que visitas en internet, lo que buscas en Google, los archivos que descargas a tu ordenador, las cosas que te gustan, las aplicaciones que instalas… Y hasta conocen tus puntuaciones en Angry Birds. Lo saben todo sobre ti. Y no puedes esconderte.

Y ésta es sólo la punta del iceberg. A la vuelta de esta página te espera un mundo dominado por el espionaje, la ciberguerra y el terrorismo. Ése es tu mundo, el que hay ahí fuera; formas parte de él, y te lo están ocultando. Demos pues por terminado este primer capítulo y este juego real: *game over*.

Ahora te enseñaré toda la verdad.

# 2

# Espionaje económico e industrial

El espionaje ha existido siempre. Con más o menos discreción, o de manera más o menos evidente, el ejercicio de espiar se ha practicado desde el origen de los tiempos, de manera que no podemos achacarlo a la tecnología.

De hecho seríamos incapaces de determinar quién fue el primer espía de la historia. Si nos atenemos al Antiguo Testamento, tendríamos que echar la vista atrás más de mil años antes del nacimiento de Cristo. Allí encontramos el curioso encargo de Josué, sucesor de Moisés y responsable de conducir al pueblo de Israel a la tierra prometida. Solicitó a dos de sus lugartenientes que acudieran de incógnito y se refugiaran en Jericó, con objeto de recopilar información útil que sirviera para el ataque que se planteaba días después sobre la ciudad. Y así sucedió, contando con la ayuda de una prostituta de nombre Rahab. Curiosamente, muchos siglos después, una de las brigadas de la República Federal de Alemania dedicada a la lucha contra la piratería y el espionaje informático recibió el mismo nombre: Rahab ¿Una casualidad? No, en lo que a espionaje se refiere, las casualidades no existen.

El gran cambio y la gran diferencia que aporta la era cibernética es que permite un espionaje masivo, sin apenas coste y, desde luego, sin riesgos. Hace tan sólo veinte o treinta años, el seguimiento de una persona era caro. Generalmente se necesitaban coches y motoristas, había que relevarlos con cierta frecuencia y se corría el riesgo de ser detectado. Los seguimientos de veinticuatro

horas eran muy complicados debido a la necesidad de personal, a las medidas de contravigilancia de la persona a la que se seguía, etc. Como consecuencia era muy limitado el número de personas a las que se podía seguir los pasos. Como veremos, hoy en día, ese tipo de espionaje forma parte, poco más o menos, de la prehistoria. Bienvenido a la era del todo vale. Bienvenido a la era del todo se puede. Pongámonos en situación.

## Era «súper», pero no tenía superpoderes

José Ignacio López de Arriortúa dice de sí mismo que es un aldeano frustrado. Que tenía buena mano cortando alcachofas con la guadaña, y también con las vacas del caserío donde nació. Que su mujer, Margari, hace el mejor bacalao a la vizcaína del mundo. Y que iba para futbolista, pero se quedó en ingeniero industrial. Bueno, eso tampoco está tan mal.

A José Ignacio todavía le recuerdan como Iñaki en Estados Unidos, pero a él le gusta que le llamen «doctor López», que es como se dirigían a él hace ya bastantes años, cuando se fue a trabajar a Alemania. Sin embargo, en nuestro país todo el mundo le conoce como Superlópez, y en la década de los noventa era uno de los grandes símbolos nacionales.

En 1993, López de Arriortúa trabajaba en la General Motors, la mayor corporación industrial del mundo. Había llegado a la empresa más de una década antes, cuando la compañía se había establecido en Figueruelas, un municipio de Zaragoza. No tardó en destacar y ascender rápidamente, hasta el punto de que, en 1993, ya era el número dos de General Motors. Antes de eso había trabajado en Alemania, donde revolucionó las relaciones comerciales con los proveedores en Opel, filial de la compañía. Eran tantas las ganancias que López le había procurado a su empresa, que fue llamado a trabajar en las instalaciones centrales de General Motors, en Detroit (Estados Unidos), y nombrado vicepresidente y director de compras.

En España, la prensa se deshacía en elogios hacia este ejecutivo nacido en Amorebieta (Vizcaya) que había llegado al techo del mundo de la industria y se codeaba con celebridades de la escena internacional. López de Arriortúa se había convertido en el hombre cuyo destino anhelaban todos los padres para sus hijos, en unos años en los que los españoles todavía creían que ir a la universidad abría de par en par las puertas del éxito laboral.

Pero Superlópez tenía un sueño. Un sueño que le acabaría trayendo problemas. Desde luego, no era un sueño tan ambicioso como el de Martin Luther King, era una aspiración más modesta y, en cierto modo, prosaica, pero era su obsesión. Y él la creía

revolucionaria. López llevaba años desarrollando un proyecto al que llamaba «Planta X». Tras los éxitos que había cosechado recientemente para General Motors, el ingeniero creyó estar en disposición de pedir algo a cambio, y quiero decir algo más que el generoso sueldo que recibía por su trabajo. Decidió que había llegado la hora de sentarse delante del presidente de la compañía y presentarle su plan. Y así fue. En 1991, Superlópez entró en el despacho de Jack Smith y le explicó su proyecto para construir una planta de fabricación de automóviles en su pueblo natal, Amorebieta, con la que esperaba dar empleo a unas cuatro mil personas.

Pero, como explica Nacho García Mostazo en su genial libro *Libertad vigilada*, el ingeniero vasco sólo consiguió salir de la reunión con la vaga promesa verbal de que General Motors estudiaría construir la planta, y no con el acuerdo cerrado como esperaba.

Poco después, López de Arriortúa voló a Zúrich para asistir a una de las reuniones que regularmente celebraba General Motors Europa. Era un trayecto rutinario, pero aquella vez ocurriría algo diferente. Antes de regresar a Estados Unidos, se detuvo en Frankfurt, donde una persona muy importante, alguien que iba a cambiarle la vida, le esperaba en un hotel. Se trataba de Ferdinand Piëch, nieto del fundador de Porsche y presidente de Volkswagen. El fabricante de coches alemán no pasaba por su mejor momento y necesitaba un plan magistral y un buen golpe de efecto; necesitaba, de hecho, a alguien como Superlópez. Piëch estaba a punto de hacerle al de Amorebieta una oferta que no podría rechazar. Era la oportunidad de su vida: la Planta X hecha realidad.

Así que el español telefoneó a su jefe en Detroit y le anunció que abandonaba la empresa. Sin embargo, su jefe, Jack Smith, no estaba dispuesto a rendirse tan pronto. Una vez de vuelta en Estados Unidos, López recibió en su casa la visita del presidente de General Motors, que venía acompañado de varios ejecutivos más de la empresa. Le pidieron disculpas por no haber sabido valorar la importancia de la Planta X, y le aseguraron que volverían a considerar la construcción del proyecto si permanecía en la compañía.

López estaba desconcertado, así que llamó por teléfono a Ferdinand Piëch, quien le sugirió que se quedara un año más en General Motors para pasarse después de ese tiempo a Volkswagen. Poco después, Superlópez recibió, de manos de un abogado de la compañía, el nuevo contrato que había de firmar con General Motors. El acuerdo establecía un ascenso que le convertiría en uno de los ejecutivos más importantes de Estados Unidos, pero también contenía una cláusula que le ligaba a la empresa por un mínimo de cinco años.

López entendió entonces que la empresa había perdido la confianza en él. Intentaban encerrarle en una jaula de oro. A pocas horas de que tuviera lugar la rueda de prensa donde debía anunciarse el ascenso del español en General Motors, el presidente Smith recibió una nota en la que Superlópez le anunciaba su marcha. «Es la acción más valiente de mi vida, Jack, perdóname y trata de entenderlo», le pedía.

Sólo un día después, López viajaba a Alemania, donde fue nombrado director de compras y de optimización de la producción de Volkswagen. Y algunos de sus colaboradores más cercanos en General Motors y Opel le acompañaron en su nueva andadura profesional. En ese momento, López todavía creía que había dado el paso más importante de su carrera. Lo que no sabía es que estaba a punto de dar comienzo un periplo judicial que se prolongaría durante varios años.

Inmediatamente, a López le notifican que Opel ha presentado una demanda ante la fiscalía de Darmstadt (Alemania) por espionaje industrial. La policía registra su despacho y su casa, así como las de sus colaboradores, y se incauta de gran cantidad de documentos que podrían incriminar al ingeniero español. Mientras tanto, López continúa trabajando para Volkswagen, desarrollando el plan para el que ha sido contratado. Sin embargo, tres años después, la vorágine de demandas y acusaciones había alcanzado su punto álgido.

El Gran Jurado del Tribunal Federal de Detroit acepta a trámite una demanda de General Motors y Opel contra López y Volkswagen. Se les acusa de violar una decena de leyes estadounidenses, imputándoles delitos de «sustracción y explotación ilegales de

derechos secretos empresariales ajenos», «acuerdos conspirativos para actos lesivos» y «conspiración criminal». Lo cierto es que los acusados saben que sus demandantes no cuentan con pruebas sólidas que puedan sustentar sus acusaciones, pero las cosas van empeorando. Existen insistentes rumores de que la fiscalía de Darmstadt, que instruye el caso contra López desde hace tres años, está a punto de presentar un pliego de acusaciones bien fundadas contra él, lo que lleva a Superlópez a anunciar su dimisión el 29 de noviembre de 1996.

Y así ocurrió, sólo dos semanas después de renunciar a su empleo en Volkswagen, la fiscalía presenta cargos contra López de Arriortúa por espionaje industrial contra General Motors. La fiscalía, en un caso sin precedentes, había tomado declaración a 196 testigos, revisado 23.000 folios de actas y analizado el contenido de disquetes y cintas confiscadas que llenarían 2,25 millones de páginas si se imprimiesen. Ferdinand Piëch y López saben que hay caso, y que es muy probable que se resuelva con una sentencia condenatoria.

Parecía que General Motors tenía asegurada su victoria en los tribunales. Sin embargo, en un giro inesperado de los acontecimientos, los abogados de Volkswagen consiguen llegar a un acuerdo con el gigante estadounidense para resolver el asunto fuera de los juzgados. Los alemanes se comprometen a pagar cien millones de dólares a General Motors, así como a adquirir componentes de la compañía por valor de mil millones de dólares a lo largo de un periodo de siete años. A cambio, los norteamericanos retiran la demanda. Pero ¿cómo es posible que General Motors haya aceptado ese trato si la indemnización judicial podía haber ascendido a 7.000 millones de dólares, haciendo quebrar a Volkswagen, su gran competidor? Aquí empieza la segunda parte del caso Superlópez. La parte en la que se explica todo.

A pesar del acuerdo alcanzado entre los dos gigantes de la automoción, las leyes dictan que la investigación judicial en Alemania debe proseguir adelante. López tendrá que sentarse en el banquillo de los acusados. La vida se le ha complicado en los últimos años al ingeniero vasco, pero todavía no ha llegado lo peor. Unas

semanas antes de la celebración del juicio en Darmstadt, López sufre un grave accidente de tráfico en la A-1, en la provincia de Burgos. El coche en el que viaja colisiona con un camión y resulta gravemente herido. Tan grave que permanecerá tres meses en coma.

La fiscalía alemana decide entonces sobreseer el caso e imponer a Superlópez una multa de 400.000 euros, en previsión de que pasará mucho tiempo hasta que esté en condiciones de declarar en un juicio. Los médicos dicen que ha sufrido lesiones cerebrales que pueden ser irreparables.

Pero, si los problemas de salud de López son acuciantes, sus problemas judiciales también distan mucho de poder resolverse. El Gobierno de Estados Unidos quiere reabrir el caso por espionaje industrial en Detroit y solicita a España la extradición del ingeniero. Nuestro héroe patrio podría enfrentarse a cinco años de prisión y una multa de 60.000 dólares. Finalmente, la Audiencia Nacional deniega la extradición aduciendo las lesiones cerebrales del procesado, que acusa pérdida de memoria.

Pero lo curioso del caso son los cargos que el Departamento de Justicia estadounidense trata de imputar a López. Cuatro de los seis cargos que formula son por «fraude mediante el uso de comunicaciones por cable o electrónicas». Es por ello que el abogado de Superlópez se pregunta: «¿Qué delito es hablar por teléfono o por vía telegráfica?». Y no sólo eso. Los cuatro registros telefónicos que menciona la acusación se produjeron antes de que López fuera demandado ante los tribunales, y, sorprendentemente, tres de ellos tuvieron lugar antes incluso de que se hubiera marchado de General Motors a Volkswagen.

¿Por qué y cómo tenía el Gobierno de Estados Unidos escuchas telefónicas de López de Arriortúa antes de que éste pudiera haber cometido ningún delito? Los abogados del español y de Volkswagen comienzan a sospechar que la NSA pueda haber intervenido las comunicaciones del español durante el tiempo que estuvo trabajando para General Motors, bien porque lo consideraba una acción necesaria de cara a garantizar la seguridad económica nacional, bien como parte de un proceso rutinario de espionaje.

Curioso, ¿verdad? Hasta esa fecha, el espionaje preventivo, concepto que hoy está instaurado con normalidad en nuestra sociedad, no era conocido. El alto coste del seguimiento que mencionaba antes hacía que no se pudiera espiar a grandes cantidades de personas al mismo tiempo, por lo que se buscaban objetivos reales e inmediatos. Ése no parecía el caso de Superlópez. ¿Qué había ocurrido?

Con estos datos empezaba a cobrar sentido el acuerdo alcanzado entre General Motors y Volkswagen. De este modo, López y el fabricante alemán zanjan el asunto fuera de los tribunales con una multa de cuantía inferior a la que habría impuesto un juez. Y, por otro lado, no se pone al descubierto que General Motors ha obtenido pruebas por primera vez por medio de escuchas ilegales masivas en las que está implicado el propio Gobierno de Estados Unidos.

Superlópez queda libre. Pero su leyenda se ha desvanecido con el tiempo. El ejecutivo superhéroe que conquistó a los españoles, tristemente, no tenía superpoderes. No sólo había estado a punto de morir, sino que había arruinado su carrera por enfrentarse a un rival mucho más fuerte que él: la terrible NSA, es decir, el brazo ejecutor del Gobierno de los Estados Unidos de América. Un rival que, si ya parecía tener algún superpoder en los años noventa, había empezado a desarrollar algo que ha ido perfeccionando hasta extremos inimaginables; la «superaudición». Hoy puede verlo todo, y de hecho lo hace. Puede oírlo todo, y de hecho pocas cosas se le escapan; y, además, lo lee y lo almacena todo. En cualquier momento. En cualquier lugar.

## El amigo americano: ¡tener amigos para esto!

El caso Superlópez había dado mucho de qué hablar en España, pero ése no es el único motivo por el que he decidido abrir el capítulo sobre espionaje industrial con este protagonista. Industria del automóvil al margen, este caso es un ejemplo perfecto para entender el gran cambio que produce el espionaje en el mundo empresarial. Se trata de un espionaje multinivel, que tiene lugar tanto en el plano horizontal como en el eje vertical. En el plano horizontal tenemos un espionaje de carácter industrial, que tiene lugar normalmente entre empresas competidoras.

Sin embargo, encontramos otro tipo de espionaje, de carácter vertical, en el que los gobiernos intervienen directamente en las actividades empresariales, bien para favorecer a las compañías de sus países, bien para evitar que la industria nacional sea perjudicada por la intervención, honesta o no, de un segundo Estado o empresa, bien para garantizar la seguridad económica de la nación. La segunda parte del caso Superlópez es un ejemplo de este segundo modelo, con el Gobierno de Estados Unidos obteniendo, almacenando y filtrando a placer escuchas ilegales para favorecer o defender a una empresa nacional frente al espionaje industrial de una compañía extranjera.

Es decir, en el caso Superlópez están involucradas las dos formas de espionaje de forma simultánea. Y no es un hecho aislado. Lo cierto es que sucede desde aquel momento con mucha más frecuencia de la que pensamos, hasta el punto de que la línea que separa los gobiernos de las empresas de bandera es a veces imperceptible.

Con la caída del muro de Berlín y el fin de la guerra fría, los sistemas de escucha y vigilancia de Estados Unidos y sus aliados fueron rebajando su carácter militar, abriéndose paso de forma progresiva en el terreno económico. En realidad, este cambio de enfoque venía gestándose desde 1970, cuando el Consejo Asesor de Inteligencia Exterior de Estados Unidos recomendó que se considerase «el espionaje económico un aspecto de la seguridad

nacional, con un grado de prioridad equivalente al espionaje diplomático, militar o tecnológico».

Con ese fin, la NSA, la CIA y el Departamento de Comercio de Estados Unidos crearon la Oficina de Enlace de Inteligencia, cuya misión era «gestionar el espionaje exterior de interés para el Departamento de Comercio».

Para llevar a cabo la nueva tarea de vigilancia económica, Estados Unidos y los otros «cuatro ojos», los aliados que conforman la alianza UKUSA, tenían a su disposición la maquinaria perfecta, una herramienta de la que ya hemos hablado: se trataba de la red Echelon.

El de Superlópez no es un caso aislado al que hacemos referencia por la cercanía del personaje, ni un elemento folclórico de espionaje español. El caso forma parte de toda una investigación llevada a cabo por la Unión Europea sobre el espionaje masivo practicado por Estados Unidos.

En esa época estaba de actualidad el informe Campbell, que se le había encargado al Parlamento Europeo. Pues ese documento abriría paso a la mayor investigación pública sobre Echelon, y el caso Superlópez aparece recogido en él. Por supuesto, la investigación contó con incontables trabas, debido a la presión que Estados Unidos ejerció sobre sus aliados europeos para que el informe no viera la luz.

Pero vio la luz. En 1998, el Parlamento Europeo iba a celebrar un debate sobre vigilancia electrónica y tecnologías de control político. En aquellos años, casi nadie sabía nada sobre estos asuntos, y los diputados europeos no eran una excepción. Así que la Eurocámara decidió encargar un informe a la Fundación Omega, que se dedicaba a hacer estudios de mercado, para instruir a los parlamentarios sobre el tema que centraría el debate.

El informe no era más que un borrador de trabajo, pero contenía suficientes revelaciones sobre el alcance del espionaje gubernamental como para que el Parlamento Europeo decidiera ampliar el estudio sobre el uso de medios de vigilancia política. Fue

así como contactó con Duncan Campbell, el mayor experto mundial en Echelon.

En el año 2000, Campbell expuso su informe ante la Eurocámara, en una sesión abierta a los medios de comunicación. Lo que los presentes escucharon aquel día en la sala removió los mismos cimientos de la Unión Europea. Echelon era una realidad. No era una película de espías, ni el producto alocado de una imaginación paranoica. Echelon era la red de espionaje más grande del mundo y tenía capacidad para interceptar 2.000 millones de comunicaciones privadas diarias. Algo inimaginable que daba una enorme ventaja al que desde entonces podemos considerar como el «Gran Hermano»: el Gobierno de los Estados Unidos de América.

De hecho había multitud de pruebas que determinaban que no se estaba utilizando únicamente la red por motivos de seguridad, sino que, una vez desarrollada, la tecnología se estaba empleando para interceptar las comunicaciones de empresas y poder intervenir así a favor de sus compañías nacionales. Por ejemplo, Campbell contaba cómo, «en 1994, la NSA interceptó llamadas telefónicas entre Thomson-CSF (una empresa pública francesa de electrónica militar) y el Gobierno de Brasil en relación con SIVAM, un sistema de vigilancia vía satélite, de 1.300 millones de dólares, para la selva amazónica. Esta empresa había sobornado presuntamente a miembros del comité de selección del Gobierno brasileño. Sin embargo, ¡qué mala suerte!, finalmente, el contrato se adjudicó a la empresa estadounidense Raytheon Corporation, que posteriormente declaró que «el Departamento de Comercio trabajó intensamente en este proyecto en apoyo de la industria estadounidense». Casualmente, Campbell desveló que la empresa Raytheon Corporation trabajaba en el mantenimiento de los satélites de Echelon que la NSA tiene en Sugar Grove, y tenía pocas dudas de que la compañía se había valido del sistema de espionaje del Gobierno estadounidense para obtener ventajas en la negociación con el Gobierno brasileño.

Hoy entendemos ese agradecimiento, así como el verdadero sentido de la expresión «trabajar intensamente». De hecho, en los próximos capítulos verás hasta qué punto han mejorado y

perfeccionado su «trabajo». En la actualidad, Echelon es a las herramientas de la NSA lo que el primer avión conocido es a un actual transbordador espacial.

Y hoy conocemos muchas historias de espionaje económico parecidas. Ese mismo año, Airbus perdió un contrato de 6.000 millones de dólares con Arabia Saudí en favor de las empresas estadounidenses Boeing y McDonnell Douglas. El informe Campbell destapó que «la NSA interceptó todos los faxes y llamadas telefónicas transmitidos a través de un satélite de telecomunicaciones comercial entre el consorcio europeo Airbus, la compañía aérea nacional saudí y el Gobierno de Arabia Saudí. La agencia pasó la información a los funcionarios estadounidenses que presionaban a favor de la oferta de Boeing Co. y McDonnell Douglas Corp., que acabó por adjudicarse el concurso».

La rivalidad entre Airbus y Boeing es conocida, y aquél no sería el último escándalo de espionaje económico que rodearía a su competencia comercial. Unos años después, en 2003, el presidente ejecutivo de Boeing, Phil Condit, dimitiría por otro caso de espionaje durante el concurso lanzado por la Fuerza Aérea estadounidense (Air Force) para adquirir una nueva flotilla de aviones cisterna. Boeing, que competía en el concurso con Airbus, recibió información confidencial desde la Fuerza Aérea sobre la oferta que había realizado el gigante europeo. Al frente de la unidad de adquisiciones de la Fuerza Aérea estaba Darleen Druyun, considerada entonces como una de las mujeres más poderosas en el Pentágono. Ella filtró la información confidencial desde la Fuerza Aérea sobre los términos de la oferta de Airbus, que permitió a Boeing hacerse con un contrato valorado en 22.000 millones de dólares más otros 5.000 millones de mantenimiento. Vistos estos ejemplos y estos contratos perdidos, casi parece un milagro que el consorcio europeo Airbus siga hoy en pie, teniendo rivales tan duros en la lucha por sus contratos. Y no, no me refiero a Boeing precisamente.

Cuando el Parlamento Europeo supo que Estados Unidos estaba interviniendo mediante escuchas secretas en los contratos comerciales que afectaban a empresas europeas, muchos se escandalizaron primero, y después montaron en cólera. El grupo

parlamentario de los Verdes pidió una comisión de investigación sobre Echelon, pero, sorprendentemente, de los quince miembros que componían entonces la Unión Europea, sólo Alemania y Francia se pronunciaron a favor de su apertura.

O no tan sorprendentemente. El Gobierno estadounidense, entonces presidido por Bill Clinton, inició una campaña diplomática para presionar a sus aliados europeos con el fin de que la comisión de investigación no saliera adelante. Todos los parlamentarios británicos se opusieron a su creación, así como el Partido Popular Europeo, que adujo presiones de Estados Unidos. Este hecho es una de las grandes vergüenzas de la Unión Europea, en la que es evidente que las presiones de Estados Unidos a los países miembros han evitado incluso que estos defiendan sus derechos fundamentales, impidiendo que los ciudadanos conozcan la verdad. Además de las presiones norteamericanas, en todas estas acciones de *lobby*, o grupo de presión, hemos de dar un papel significativo al Reino Unido, al que casi podemos calificar como una filial de Estado Unidos que defiende sus intereses en el mismo corazón de Europa.

Finalmente, la comisión de investigación no salió adelante, pero sí se aprobó una «comisión temporal», con el cometido de comprobar si son necesarias medidas extraordinarias de encriptación para asegurar las comunicaciones en Europa y «determinar si la industria europea está expuesta a riesgos como consecuencia de la interceptación global de las comunicaciones».

El portavoz de la Comisión Europea, Jonathan Faull, quiso tranquilizar los ánimos con unas declaraciones en las que afirmó que el sistema de encriptación de la Unión Europea, que fabrica Siemens, es seguro. Tan seguro, añadió, que es el mismo que han elegido «los Estados miembros de la Unión Europea y los de la OTAN». Sin quererlo, Faull había encendido todas las alarmas. ¿Había dicho la OTAN? ¿El sistema de encriptación de señales de la Unión Europea era el mismo que el de Estados Unidos? Aquello acrecentó aún más la desconfianza de los parlamentarios europeos, que empezaban a estar seguros de que la NSA había puesto bajo su vigilancia las instituciones comunitarias. Por supuesto, no se equivocaban.

La Comisión Europea decidió entonces reforzar la seguridad de sus comunicaciones, algo que era una tarea pendiente desde hacía tiempo. De hecho, fue una de las primeras tareas a las que hubo de hacer frente Javier Solana cuando pasó de la secretaría general de la Alianza Atlántica (OTAN) a ser el alto representante de Política Exterior y Seguridad de la Unión Europea. Al parecer, ni siquiera el edificio del Consejo de Ministros reunía las mínimas condiciones para garantizar la seguridad y la privacidad de las comunicaciones, y la Alianza Atlántica les había advertido de que «no les enviarían ni siquiera una tarjeta navideña mientras no acondicionaran el recinto».

Pero, más allá de las deficiencias de seguridad de las comunicaciones que puso de manifiesto la Comisión Echelon, lo que quedó patente es que Estados Unidos había tejido una red de espionaje masivo mundial de la que nadie, ni siquiera los aliados o los ciudadanos anónimos, estaba a salvo. Eso nos lleva a la primera cosa que debemos preguntarnos. ¿Por qué? Es decir, ¿por qué los norteamericanos espían a los que consideraban sus amigos y aliados? Nuestra primera respuesta es simple. Hay dos motivos fundamentales.

El primero es sencillo: porque pueden. Nadie más tenía esa tecnología; y la ventaja tecnológica que aún hoy tiene Estados Unidos es poder. El poder en manos del Gobierno estadounidense y de su temible agencia, la NSA, es sinónimo de abuso, aunque, según ellos, «por el bien del país», lo que en realidad es atribuirse absoluta libertad para poder campar a sus anchas por el mundo.

El segundo motivo tampoco es complejo. Lord Palmeson, primer ministro británico en el siglo XIX, pasó a la posteridad por su pragmática frase «Inglaterra no tiene amigos ni enemigos. Inglaterra tiene intereses». Pues bien, siglos después, el Gobierno de los Estados Unidos de América ha desarrollado hasta el extremo ese razonamiento.

Echelon recopila información económica sobre empresas, la cual facilita después a compañías norteamericanas para favorecer su posición en el mercado global. Ni siquiera las asociaciones sin ánimo de lucro están a salvo de los tentáculos de la NSA. Organizaciones

no gubernamentales como Amnistía Internacional, Cruz Roja o Greenpeace son objetivos permanentes de los sistemas de escucha de Echelon.

Ante las evidencias destapadas por la Comisión Echelon, Estados Unidos trató de salir al paso de las acusaciones y justificar su actuación. El director de la CIA en el año 2000, George J. Tenet, aseguró que «hay casos en los que nos enteramos de que empresas extranjeras, o bien sus gobiernos, sobornan, mienten, estafan o engañan para arrebatar licencias a empresas estadounidenses. Cuando obtenemos esta información, la transmitimos a las agencias correspondientes, advirtiéndoles al respecto. Éstas utilizan esa información a través de otros medios y canales para comprobar si pueden ayudar a una empresa estadounidense. Lo que hacemos es defendernos, nunca atacamos y nunca atacaremos».

Estados Unidos se defiende. Nunca ataca (¡ejem!). O eso asegura. Sin embargo, el Parlamento Europeo desconfía de los estadounidenses. Unos cuantos casos aislados de corrupción no justifican el espionaje masivo. Y la corrupción se combate desde la legalidad. A pesar de todo, Estados Unidos dice estar dispuesto a colaborar, y, para demostrar su buena fe, autoriza unas pocas reuniones de parlamentarios europeos con autoridades estadounidenses para hablar sobre Echelon. Se conciertan citas con miembros del Departamento de Estado, del Departamento de Comercio, de la CIA y de la NSA.

La delegación europea viajó a Washington en mayo de 2001 para recabar información y poder llevar a cabo esas reuniones, pero, sorprendentemente, la mayoría de los encuentros previstos nunca se celebraron: fueron anulados a última hora con excusas muy poco convincentes, ahondando la brecha de desconfianza que se había abierto entre Estados Unidos y la Unión Europea.

Las conclusiones de la comisión temporal Echelon pusieron de manifiesto la necesidad de mejorar la seguridad de las comunicaciones, y determinaron la existencia de una red de espionaje masiva protagonizada por Estados Unidos y Reino Unido que levantó muchas ampollas en Europa, especialmente en Alemania y Francia. Pese a todo, aunque son los primeros de la clase, no

puede decirse que Estados Unidos y sus socios del «Club de los cinco ojos» tengan la exclusiva del espionaje económico mundial.

Todo lo anterior ha puesto de relevancia que tras Echelon entramos en un nuevo escenario. El espionaje y el sabotaje industriales ya no eran sólo una cosa entre empresas: los gobiernos, por su interés geoestratégico, participan en él. Eso crea situaciones de compleja resolución para determinadas empresas. Una compañía que debe proteger sus sistemas puede hacerlo hasta cierto punto, pero, por muy extrema que sea su vigilancia, será difícil que pueda protegerse contra los recursos casi ilimitados y los enormes tentáculos de los servicios de inteligencia de determinados países.

Por otro lado, podríamos afirmar que es más fácil atacar una empresa que defender todas las que un país posee. Por ese motivo, es fundamental la concienciación sobre la seguridad informática, y se debe procurar que las empresas que trabajan con datos y material sensible cuenten con una protección adecuada en sus sistemas. No sólo se está poniendo en juego el robo de información y de secretos industriales, sino que el propio patrimonio de las personas y las empresas puede estar comprometido (por ejemplo, con la intromisión en los sistemas informáticos de los bancos).

En un mundo idílico, pretenderíamos que «papá Estado» tuviera la capacidad de proteger a todas sus empresas de ataques exteriores que pusieran en riesgo el sistema, pero eso, hoy, es poco factible. Se puede entrar en todos los dispositivos que estén conectados. Todos. El riesgo es absoluto. Lo único que se puede hacer es contar con expertos que monitoricen veinticuatro horas al día los sistemas, que instalen cortafuegos y que trabajen diariamente en testear la calidad de los mismos. Eso no lo puede hacer el Gobierno, ni las fuerzas y cuerpos de seguridad del Estado. Cada país necesita crear un tejido de empresas de seguridad informática con personal convenientemente formado y dotadas tecnológicamente para defender su tejido empresarial. De hecho, por ley, determinado tipo de compañías deberían estar obligadas a contar con los servicios de estas empresas, y esto no debería ser una opción, ya que su dejadez pondría en riesgo el sistema. Un gran banco nacional puede ser una compañía privada, pero un ataque

contra ese banco que cree el caos y logre una importante fuga de capitales, por ejemplo, entabla una situación de riesgo sistémico. No debe estar en manos de empresas privadas la decisión del grado de protección más adecuada, ya que puede caer en la tentación de ahorrar en recursos en seguridad informática, o de poner en manos de personal no formado (por ejemplo, el mismo responsable tradicional de seguridad física de la compañía) la protección de sus sistemas.

Éste es un punto de inflexión. Cada país debe construir su tejido de seguridad que dé servicio a sus compañías críticas, donde el riesgo de guerra económica es real. Posiblemente, el país que mejor ha entendido esta necesidad sea Estados Unidos. Al calor de grandes contratos públicos han surgido decenas de empresas de seguridad de bandera que, si bien captan clientes e ingresos en todo el mundo con los que financian sus actividades, son sistémicas. Nacieron por la necesidad de protección de las compañías estadounidenses. Sería cómodo para un país como el nuestro depender de estas grandes corporaciones del otro lado del Atlántico. Pero en un universo virtual en el que no hay amigos ni aliados, tan sólo intereses económicos, sería una aberración y señal de que no hemos aprendido nada.

## El día que los chinos se colaron hasta la cocina en Alcobendas

En España existen algunas (pocas) empresas de seguridad que pueden dar este tipo de servicios con medios adecuados. Yo destacaría S2 Grupo, S21sec y Eleven Paths. Tienen interesantes centros de datos y cientos de empleados formados, y de ellas dependen los sistemas de la mayor parte de los bancos, las empresas energéticas, las líneas aéreas y de todo tipo de grandes corporaciones nacionales que podríamos calificar como sistémicas — y que, por lo tanto, reciben ciberataques de delincuentes comunes, de otras empresas y, también, diariamente, de agencias de otros países.

Una de esas empresas, S21sec, pasó en 2014 una situación económica complicada, y tuvo que acudir a una ampliación de capital para poder continuar con sus actividades. Pese a la importancia geoestratégica de la empresa, no fueron inversores institucionales, ni tan siquiera españoles los que acudieron a ella sino una empresa portuguesa, Sonae.

Tras ello, la mayoría de las acciones de S21sec pasó a manos portuguesas por un par de millones de euros. Eso sería impensable en otros países occidentales, que no hubieran permitido jamás que una empresa de otro país tomara control, ni tan siquiera una mínima participación, en empresas clave para la defensa electrónica. De hecho, como país, España tenía decenas de opciones para evitar que esto ocurriera, desde el Instituto de Crédito Oficial (ICO) hasta la Sociedad Estatal de Participaciones Industriales (SEPI), desde contratos públicos hasta proyectos para ministerios. Sea como fuere, hoy, algunas de las principales compañías del Ibex 35 están protegidas por una empresa, muy eficiente por otro lado, pero de capital mayoritariamente portugués.

Por supuesto, no sólo hay que cuidar estas empresas, ni proteger únicamente los sistemas informáticos. Además hay que proteger físicamente los centros de datos donde se almacena toda la información y se encuentran todos los servidores.

Uno de los centros críticos en cuanto a infraestructura tecnológica está en la granja de servidores que Telvent, hoy filial de Schneider Electric, posee en Madrid. Por la tipología de sus clientes y la información que allí se utiliza, ése es uno de los centros clave a proteger en España. Me consta que el edificio tiene unos protocolos de seguridad que, en mi opinión como usuario, son demasiado estrictos, pero que, como instalación crítica, resultan a todas luces insuficientes. Durante años una de mis empresas tuvo *racks* de servidores allí, y tuve que acudir en no pocas ocasiones al edificio. Verlo es un espectáculo, pero los protocolos de seguridad para introducir material o, simplemente, para entrar en el edificio, al menos para mí, que no trabajaba con secretos nucleares, eran poco operativos y, con perdón, un auténtico coñazo. Ahora bien, aunque no andábamos por allí como Pedro por su casa, una vez que entrabamos en el edificio el control que había sobre nuestras actividades tampoco es que fuera extremo. Dejémoslo en que cualquier cliente podría acceder a cosas que no debe ni le incumben, pero bueno.

Si la seguridad de los datos, del centro y de los servidores, por la información que se maneja, es crítica, debería serlo también la de los alrededores del edificio. Y esa parte debería estar en manos de las fuerzas de seguridad del Estado. Jamás vi un coche de policía en la puerta —igual hacen rondas de vez en cuando, pero, desde luego, no están allí—. Lejos de estar aislado y con un razonable perímetro de seguridad, el edificio de Telvent en Alcobendas está en un pobladísimo polígono industrial. Puedes aparcar prácticamente en la puerta. Eso lo hace blanco fácil para muchas cosas.

De hecho, aunque no haya trascendido hasta hoy, ya lo ha sido. Hace algún tiempo, un empleado de una empresa cercana llamó alarmado al Centro Nacional de Inteligencia (CNI) y a la policía. Habían detectado una furgoneta blanca sin ventanas que llevaba aparcada varios días en la puerta del edificio. En ella se observaba un intenso uso de aparataje electrónico y varias personas de origen asiático que entraban y salían de la misma cada equis horas. En ocasiones, había actividad las veinticuatro horas del día.

Llegar por la carretera de Burgos con coches de policía atronando con sus sirenas en dirección al edificio no suele ser la manera de resolver estas situaciones. Al ser alertados de la llegada de la policía, los ocupantes de la furgoneta arrancaron y se fueron, y nadie jamás les identificó, ni se supo qué había dentro de esa furgoneta. Aún hoy, hasta donde yo sé, no existe un perímetro de seguridad frente al edificio.

¿Qué pudo pasar? Esa furgoneta, más que posiblemente, estaba interceptando las comunicaciones de las redes internas de Telvent y del edificio. Posiblemente había estado robando y recabando datos para luego ser analizados. Y lo habían hecho con una facilidad pasmosa. Si habían logrado comprometer los sistemas, y si habían hecho un buen trabajo, posiblemente no tuvieran que volver por allí físicamente jamás, y habrían instalado dentro de sus objetivos lo necesario para operar en remoto.

Meses después, Schneider, la matriz de Telvent, tuvo que responder ante la evidencia. En Canadá se descubrió que sus sistemas en ese país, y también en España y Estados Unidos, habían sido comprometidos y atacados por hackers chinos. Habían entrado en sus sistemas e instalado *malware*. La preocupación sobre las infraestructuras críticas fue mayúscula. Habían atacado los sistemas SCADA de Telvent, utilizados por empresas e instalaciones críticas: compañías eléctricas, petroleras, de transportes y de aguas en los citados países.

Los medios utilizados, la capacidad de movilizar equipos de manera física en estos países para sus operaciones y el objetivo del ataque hacen pensar en una operación de inteligencia china para el robo de propiedad industrial y análisis de la información sobre los sistemas de estos países. En caso de un ciberataque, por ejemplo, y como veremos más adelante, uno de los objetivos básicos es la energía, pues «apagar» un país o una ciudad es una enorme ventaja competitiva.

Los responsables de Telvent poco lograron decir: «Telvent es consciente de un fallo de seguridad de su red corporativa que ha afectado a algunos archivos de clientes. Estos han sido informados y están tomando las medidas recomendadas, con el apoyo de nuestros

equipos. Telvent está trabajando activamente con la policía, los especialistas en seguridad y sus clientes afectados para garantizar que la brecha se ha contenido».

Vamos, que bla, bla, bla… Los chinos habían entrado hasta la cocina y se habían hecho con todo lo que habían querido. Estas situaciones deberían ser suficientes como para que, en los centros de datos donde concurren y se protegen instalaciones críticas, la seguridad se tome mucho más en serio, así como para que hubiera una desbandada de clientes institucionales si esto no fuera así en algún datacenter. No sé cómo se habría manejado todo aquello en Estados Unidos o en Canadá, pero en España nos habíamos dado cuenta de que «algo se cocía» y, lamentablemente, ni la policía ni el Centro Nacional de Inteligencia (CNI) controlaron la situación.

Tras el incidente de la furgoneta, tampoco llego a comprender cómo no se revisaron los sistemas en España y cómo no se identificó que estaban comprometidos. Tuvimos que esperar a la voz de alarma canadiense tiempo después. En fin.

Por cierto, resulta curioso que el tema jamás se comentara ni publicara en España, y que se descubriera meses después en Canadá, desde donde se hizo público. ¿No nos enteramos, o tenemos la malsana costumbre de ocultarlo?

## *Oh là là*: la maldición del último euro

Nuestros amigos los franceses, que pusieron el grito en el cielo cuando se destapó el informe Campbell, tienen sobrados motivos para guardar silencio cuando se habla de espionaje económico.

Tal como relata James Adams en *La próxima guerra mundial*, ya en 1993, un memorándum francés dirigido a diplomáticos galos en Estados Unidos cayó en manos de la CIA. El documento, que después se comprobó que provenía de la Dirección General de Seguridad Exterior (DGSE), la agencia de inteligencia exterior de Francia, contenía una lista de personas y objetivos empresariales a espiar, así como la información a robar. El memorándum, que constaba de veintiuna páginas, incluía ordenadores, artículos electrónicos, telecomunicaciones, armas nucleares, aeronáutica, productos químicos, bienes de consumo y de capital, materias primas y contratos importantes en el sector civil. Es decir, contenía de todo, lo cual ponía de manifiesto la existencia de un plan integral de espionaje francés.

Una de las compañías citadas en el documento era Hughes Aircraft, que casualmente había perdido un contrato de varios cientos de millones de dólares en Oriente Medio frente a una empresa francesa, lo cual desató la indignación de la dirección de la corporación aeronáutica, así como la de buena parte del empresariado norteamericano.

Por supuesto, cuando el Gobierno de Clinton pidió explicaciones a la embajada francesa por el caso, la diplomacia gala negó todas las acusaciones y aseguró desconocer la existencia de tal documento. Sin embargo, el propio Pierre Marion, quien fuera director de la DGSE, reconoció su cometido al frente de la institución, cuya sede parisina era conocida como «*la Piscine*»: «Yo trataba de obtener documentos e interceptar comunicaciones, todo al servicio de las empresas francesas». ¿Y qué hay de los aliados? ¿Cómo justificar el espionaje a los socios políticos y militares? Marion no dejaba lugar a dudas: «En materia económica y tecnológica, no somos aliados, sino competidores».

En España sabemos muy bien de las prácticas de la inteligencia francesa, pese al silencio que se guarda históricamente sobre este tema, especialmente para no perjudicar otros ámbitos de colaboración, como la lucha antiterrorista.

Un chascarrillo habitual en determinados círculos empresariales, especialmente en aquellos que tienen necesidad de competir por suculentos contratos teniendo como rivales a empresas de origen galo, es hablar de la «maldición del último euro». Es una regla no escrita, por la que, en multitud de ocasiones, cuando una empresa española y francesa compite por un mismo contrato suele ganar la francesa con un margen de precisión asombroso, haciendo que la oferta española sea siempre un poquito más cara. «Parece que, en determinadas circunstancias, siempre conocen nuestras ofertas», llegó a comentarme, entre cervezas y con sonrisa pícara en la boca, un destacado responsable de seguridad del Ministerio del Interior. Ante mi cara de incredulidad concluyó: «Vamos, que nuestras redes [empresariales] son tóxicas. Aquí, los franceses operan como Pedro por su casa…».

No es descabellado pensar así. Ya en 2013, el director del Centro Nacional de Excelencia en Ciberseguridad (CNEC), Álvaro Ortigosa, declaraba a la Cadena Ser que estimaba que unas 1.500 empresas españolas tenían puertas traseras en sus sistemas por las que delincuentes informáticos (desde empresas extranjeras hasta servicios de inteligencia de otros países) tendrían un acceso total a sus servidores pudiendo copiar, eliminar y manejar remotamente toda la información a su antojo. Multiplica este número por diez o por veinte para calcular el número de empresas españolas que están en esa situación hoy. Y todavía nos quedaremos cortos. Lo dicho, redes empresariales tóxicas.

En este punto, algún lector bienintencionado o con una alta dosis de ingenuidad pensará que los franceses no nos harían esto; ¡si son nuestros amigos y aliados! En ese caso temo que peques de una excesiva bisoñez. Lo hacen y lo seguirán haciendo. Y no sólo con nuestras empresas, sino también al máximo nivel político.

En los peores momentos de la crisis económica, con enorme incertidumbre, y con España en el ojo del huracán como riesgo

potencial para Europa, en Francia estaban preocupados por las decisiones que pudiera tomar el Gobierno de José Luis Rodríguez Zapatero. Bueno, eso puedo entenderlo, ya que también lo estábamos muchos de nosotros. El caso es que la temible Dirección General de Seguridad Exterior (DGSE) francesa bautizó a su última criatura, un troyano complejo, con el nombre de Babar, en honor al simpático elefante inmortalizado por el dibujante francés Jean de Brunhoff. Babar tenía una misión principal en Irán, pero, de paso, se utilizó para infectar desde Francia ordenadores de altos cargos y miembros del Gobierno español, recabando información que permitiera a Francia saber qué pasos iba a dar España en relación a los problemas que se avecinaban. Esto no dice mucho de la confianza de nuestros vecinos en nuestras capacidades. La verdad es que no. Pero sí dice mucho de su capacidad tecnológica.

Un documento interno filtrado desde el Centro de Seguridad de las Telecomunicaciones de Canadá (CSTC), el contraespionaje canadiense, tras un profundo análisis, determinaba: «Estimamos, con un nivel moderado de certeza, que se trata de una operación en las redes informáticas respaldada por un Estado y ejecutada por una agencia francesa de inteligencia». Concluía el informe con el análisis de Babar que «en un momento en que España era el centro de atención, porque podía arrastrar a la zona del euro hacia el abismo, se trataba de saber qué medidas barajaba tomar su ejecutivo y en qué plazos para enderezar la situación».

A preguntas de *Le Monde*, la DGSE rehusó hacer comentarios «sobre actividades reales o supuestas». Y eso que el caso estuvo a punto de tener consecuencias políticas internas, porque Babar también se había infiltrado en ordenadores en Francia, pese a que la DGSE no está autorizada a actuar dentro de su país. Allí sólo puede hacerlo la Dirección Central de Investigación Interior. Como suele ocurrir en estos casos, el tema acabó con una bomba de humo, y no se volvió a oír hablar de ello.

Pero queda claro que los servicios secretos franceses son agresivos y proactivos para luchar por el interés y posicionamiento de sus empresas. Los españoles, no tanto. Servicios secretos como los estadounidenses, británicos, chinos y franceses son «ofensivos»,

son proactivos, buscan oportunidades y posibilidades para sus empresas, cruzan líneas rojas para ello y trabajan codo con codo con sus compañías, o bien las apoyan en silencio. Servicios como los españoles, por defecto, no aparecen, o más bien lo hacen únicamente cuando hay problemas, y con un cierto carácter «defensivo». Si hay un tema de interés nacional o un conflicto que les compete, entran en acción. Por ejemplo, en el conflicto que culminó con la expropiación del 51 por ciento de las acciones de YPF frente a Repsol en Argentina, los servicios secretos españoles invirtieron muchos esfuerzos, pero posiblemente entraron en acción tarde, cuando el problema ya era irreversible y las cartas estaban ya repartidas.

Nunca he sabido si se trata de poca capacidad operativa, es decir, de pocos medios, o de una malentendida noción de seguridad. En su descargo puedo decir que el Centro Nacional de Inteligencia cuenta con 223,6 millones de euros de presupuesto. De ellos, 19,8 millones de euros son fondos reservados, es decir, pueden ser gastados sin justificar ni dar explicaciones. Puede parecer mucho dinero, pero la realidad es que es muy insuficiente. La Casa, como la conocen sus allegados, cuesta a cada españolito de a pie 4,8 euros al año. Servicios secretos de otros países cuestan de media unos 25 euros por habitante. Con las filtraciones de Edward Snowden supimos, tras leer un documento de 178 páginas, que la CIA y la NSA contaban, en 2014, con un presupuesto anual de 52.600 millones de dólares. La comparación es odiosa, y explica por qué, cuando necesitamos algo, llamamos al «amigo americano», que tiene los programas y herramientas que nos ayudan a resolver situaciones extremas.

Pese a esa diferencia de presupuesto, un operativo del CNI me dijo en una ocasión: «No te fijes en el presupuesto oficial. Tenemos cientos de empresas para financiarnos y lograr objetivos. Si no lo hace el centro lo hará Indra o decenas de pequeñas empresas satélite alrededor».

Un buen amigo mío, al que llamaremos Klasus, miembro de los cuerpos y fuerzas de seguridad y experto en tecnología y en la lucha antiterrorista, me comentaba frustrado: «Hace años, cuando teníamos algún archivo encriptado con PGP, se lo mandábamos a los

norteamericanos. Teóricamente, ellos nos ayudaban a romper la protección. La mayoría de las veces tardaban casi un mes en contestar, y, finalmente, lo hacían diciendo que no se había podido hacer nada… Insistí varias veces a mis superiores en que dejáramos de mandarlos. La única certeza que teníamos es que ahora ellos tenían los archivos, nosotros seguíamos sin verlos, y ellos… bueno, jamás lo sabremos».

Al margen de temas presupuestarios, han sido muchas las ocasiones en que la inteligencia francesa y sus «primos mayores» los norteamericanos han protagonizado rifirrafes por cuestiones de competencia económica. A principios de los años noventa, la empresa francesa Dassault Aviation estaba tratando de desarrollar un avión de caza que fuera indetectable para los radares, para lo cual no dudó en espiar a compañías británicas y norteamericanas. Cuando el FBI descubrió que la DGSE estaba tratando de infiltrarse en la multinacional estadounidense Dow Corning, así como de comprar a trabajadores en otras veinticuatro empresas, los planes franceses se fueron al traste.

No obstante, a los ofendidos norteamericanos más les habría valido estarse calladitos. Poco después, en 1995, la CIA montó una operación para conocer las posiciones de Francia sobre ciertos temas de interés económico estratégico para Estados Unidos. Es conocido que Francia ejerce un proteccionismo importante sobre su industria cultural, poniendo trabas a la comercialización del cine estadounidense en las salas del país. La CIA quería espiar a los funcionarios galos para obtener información al respecto, habida cuenta de la importancia que la exportación derivada de la industria cinematográfica tiene para Estados Unidos. Así que envió un dispositivo a París para acometer el trabajo, pero todo resultó en una chapuza impropia de la agencia de inteligencia más famosa del mundo.

Una agente inexperta de la CIA trató de sobornar a un funcionario del Gobierno francés y fue descubierta rápidamente. La mujer se había presentado como la responsable de relaciones públicas de una empresa de Texas, pero fue desenmascarada por los servicios de inteligencia franceses, que, en lugar de destapar el

asunto, decidieron seguir el juego a los estadounidenses para ver qué podían obtener.

El empleado del Gobierno al que la CIA trató de sobornar pasó entonces a ser un agente doble. Fue enviado a reuniones con los espías norteamericanos en las que, supuestamente, él revelaba información sobre industria agraria y del espectáculo a cambio de dinero. En realidad, el presunto sobornado lo único que hacía era suministrar a la CIA la información que le dictaba la inteligencia francesa, que, de ese modo, logró descubrir a varios agentes estadounidenses, entre ellos, el jefe del espionaje de la CIA en París.

Después, Francia pidió a los agentes que abandonaran discretamente el país y llamó a consultas a la embajadora estadounidense. La chapuza de la CIA tuvo más consecuencias de las esperadas cuando se supo que ni la diplomacia ni el Congreso de Estados Unidos estaban al corriente de este tipo de operaciones, lo cual obligó a la agencia a suspender casi todas sus actividades de espionaje. Y no sólo en Francia, sino también en buena parte de Europa, a la que el Gobierno francés había puesto sobre aviso.

Otro célebre dispositivo norteamericano tenía por objetivo arrebatar a los franceses un contrato de 6.000 millones de dólares con Arabia Saudí por la venta de aviones civiles y equipamiento militar. El primer ministro francés de entonces, Édouard Balladur, estaba a punto de reunirse con el rey Fahd para cerrar el acuerdo cuando los saudíes se echaron atrás. La CIA y la NSA habían descubierto las condiciones del contrato y los sobornos pagados, lo cual permitió al Gobierno de Clinton intervenir para mejorar la oferta francesa y conseguir que el contrato de aviación fuese asignado a Boeing y McDonnell Douglas, mientras que el equipamiento militar fue adquirido a varias empresas también estadounidenses.

Pero no podemos hablar del espionaje económico protagonizado por Estados Unidos sin mencionar a su fiel aliado y escudero: el Reino Unido. La NSA y el centro de escuchas británico, el GCHQ (uno de los servicios secretos del Reino Unido), suelen colaborar estrechamente en este tipo de operaciones. Es el caso, por ejemplo, de un conocido escándalo en el que norteamericanos y británicos fueron acusados de intentar hackear las tarjetas SIM del mayor

fabricante mundial: Gemalto. Esta multinacional neerlandesa puso en marcha una investigación interna cuando descubrió que la seguridad de sus sistemas había sido comprometida, después de una serie de ataques informáticos muy complejos que tuvieron lugar durante 2010 y 2011. La investigación de Gemalto concluyó que existían «pruebas razonables de que probablemente se deben a una operación de la NSA y la GCHQ», aunque negó que los ciberataques sirvieran para robar las claves de cifrado de las tarjetas SIM. Según Gemalto, los servicios secretos sólo consiguieron acceder a la red de comunicación de sus oficinas, pero no romper la seguridad de las tarjetas.

Los resultados de esta investigación indicaban que la NSA y la GCHQ estaban detrás del robo de millones de códigos Ki de tarjetas SIM. Estos códigos Ki son los que identifican las tarjetas SIM y les permiten conectarse con sus operadores de telefonía. La NSA descubrió que era mucho más sencillo interceptar y robar estos códigos que romper sus sistemas de cifrado. Los objetivos de las agencias de inteligencia eran operadores de países como Afganistán, Yemen, India, Serbia, Irán, Islandia, Pakistán o Somalia, aunque la GCHQ también tenía objetivos de espionaje en Alemania, México, Brasil, Canadá, China, Italia, Rusia, Suecia, España, Japón y Singapur.

Lo extraño del caso Gemalto es que esta multinacional fabricante de tarjetas SIM no interpuso una sola denuncia por espionaje económico, seguramente porque sabía que no tenía nada que hacer frente a enemigos tan poderosos como los servicios secretos de Estados Unidos y el Reino Unido. Toda la investigación fue de carácter interno, y, una vez hechas públicas sus conclusiones, la compañía afirmó que no quería volver a hablar del asunto, invitando a la prensa a pasar página rápidamente. Con la ley en la mano, tal decisión es tremendamente controvertida, pero muy práctica para una compañía privada que vende una importantísima parte de su producto a empresas norteamericanas y británicas.

Nunca sabremos con certeza si la NSA y la GCHQ lograron su objetivo de espiar millones de comunicaciones a través de las tarjetas SIM de Gemalto. La empresa neerlandesa asegura que no

fue así, pero también es cierto que cuenta con buenos motivos para negarlo: en un negocio que mueve miles de millones al año, no conviene dar la imagen, ante los clientes y la competencia, de que el servicio que ofreces no es seguro. Los papeles de Snowden aseguran que los espías sí alcanzaron su objetivo. Y no olvidemos que esos papeles se filtraron directamente desde los servicios secretos norteamericanos y británicos. Blanco y en botella…

Pero el espionaje económico e industrial no sólo se produce en los confines de Occidente. De hecho, un gran número de ataques de estas características a empresas europeas y americanas proviene de Rusia y Asia. Alemania calcula que pierde cada año cerca de 12.000 millones de euros por este motivo, y una de cada dos firmas alemanas ha sido víctima en los dos últimos años de un caso de espionaje o, al menos, de un intento de piratería industrial. De estos ataques, el 38 por ciento proviene de Asia, mientras que el 32 por ciento procede de Rusia y las antiguas repúblicas soviéticas.

La preocupación del Gobierno alemán por la vulneración de sus empresas ha alcanzado niveles de alarma en los últimos años. Son los casos dirigidos desde Rusia los que plantean un especial quebradero de cabeza a las autoridades germanas, que consideran que se está poniendo en riesgo el tejido industrial del país. Y es que, si bien Rusia es el primer socio comercial de Alemania, en la última década, las empresas alemanas han sido objeto de cuantiosos robos desde ese país relativos a la propiedad intelectual de sus compañías, especialmente en los sectores de la automoción, las energías renovables, las tecnologías de la comunicación, la industria química, los equipos de rayos X y la fabricación de armas.

Por su parte, y como en el caso de Alemania, China es la causante del mayor número de ataques de espionaje económico e industrial en el Reino Unido y Estados Unidos. En 2010, en una exhibición ante el mundo de su gran poderío militar, China presentó su flamante avión de caza Chengdu J-20. Los chinos habían tratado durante años de desarrollar un cazabombardero con tecnología furtiva, indetectable para los radares, aunque sin éxito hasta entonces. Pero la nueva joya de la aviación asiática guardaba un parecido más que sospechoso con el caza furtivo estadounidense.

Pronto se descubrió el motivo. En 1999, un F-117 Nighthawk de Estados Unidos fue derribado en combate durante la guerra de los Balcanes. Algunas piezas del avión siniestrado fueron compradas después por el Gobierno de China directamente a los agricultores locales que las habían recogido, y luego fueron entregadas a empresas militares chinas para que copiaran el caza norteamericano. Además, por entonces, era algo conocido que el presidente yugoslavo Slobodan Milosevic tenía la costumbre de compartir la tecnología enemiga capturada con sus aliados chinos y rusos. Esto explicaría también el origen del prototipo T-50, del fabricante Sukhoi, que fue dado a conocer ese mismo año.

Pero el caso de espionaje económico quizá más importante protagonizado por el gobierno de China es el que recibió el nombre de «Operación Aurora». En esta ocasión, los objetivos del ataque fueron varias decenas de multinacionales, entre las que destacaba Google; pero el robo de la información empresarial no sería destinado únicamente a usos comerciales, sino también políticos.

En diciembre de 2009, diversos empleados de Google localizados en China y varios países más recibieron un extraño correo electrónico en el que se les pedía que clicaran en un enlace. Lo que los trabajadores de la compañía no sabían es que aquel clic desencadenaría uno de los ciberataques más sofisticados registrados hasta ese momento. Un troyano se descargó de forma secreta en los ordenadores infectados, instalando un programa que permitía el acceso remoto de un usuario no autorizado para robar la información almacenada. Google no fue la única víctima de este ciberataque, que golpeó a cerca de cuarenta multinacionales, entre ellas Adobe, Juniper, Rackspace, Symantec, Northrop Grumman, Morgan Stanley y Yahoo!, aprovechando para ello los llamados «*zero days*» (o «días cero», vulnerabilidades no conocidas y, por lo tanto, no parcheadas por los fabricantes del *software*).

El *malware* era tan sofisticado (utilizaba hasta ocho *zero days*, algo nunca visto antes) que resultaba casi imposible determinar quién era el responsable de la operación, pero una serie de indicios llevaron a sospechar que el Gobierno de China estaba detrás de lo sucedido. Después de un rastreo exhaustivo, la NSA llegó a la

conclusión de que los ataques provenían de dos universidades chinas que mantenían estrechos vínculos con el Ejército Popular de Liberación, rama militar del Partido Comunista Chino.

El objetivo de los ataques no era únicamente el de robar información a las grandes multinacionales para que las empresas chinas pudieran copiar y desarrollar su tecnología, sino que tenía también la intención de obtener los datos personales de millones de ciudadanos chinos para poder identificar y perseguir a opositores al régimen. Google confirmó el robo de propiedad intelectual de la empresa, así como la violación del acceso a algunas cuentas de correo electrónico de activistas de derechos humanos de China, motivo por el que decidió dejar de censurar los resultados de sus búsquedas en aquel país y trasladarse a Hong Kong, que no está sujeta a las leyes anticensura de China.

Pero el espionaje industrial y económico se produce a todos niveles, y no sólo tiene lugar entre grandes potencias como Estados Unidos, Reino Unido, Francia, Alemania, China o Rusia. Todo el mundo espía en la medida de sus posibilidades, y quien no lo hace es, básicamente, porque no puede.

También es cierto que, en contadas ocasiones, las empresas se comportan con honestidad e integridad moral, incluso cuando la tentación de robar información a la competencia es muy alta. Es lo que sucedió con Pepsi y Coca-Cola hace unos años, en 2006, cuando unos empleados de la segunda trataron de vender información a Pepsi. En este caso, Pepsi jugó limpio y descubrió a los traidores, así que la cosa no pasó a mayores. La receta de Coca-Cola sigue siendo uno de los secretos empresariales mejor guardados; sólo la conocen dos directivos, y se encierra en una cámara acorazada del Sun Trust Bank, en Atlanta.

Pero la norma es que el espionaje industrial es generalizado, y ni siquiera las empresas de países tan democráticos y respetables como Suecia se libran de ello. En 2013, por ejemplo, tres directivos de la multinacional Ikea, en su filial de Francia, fueron acusados de espiar a sus propios trabajadores. Al parecer, la compañía tenía acceso a ficheros policiales gracias a la colaboración de una empresa

de seguridad privada, Sûreté International, y comprobaba los antecedentes penales de sus empleados y clientes. Ikea no sólo estaba al corriente de las prácticas de sus directivos en la filial gala, sino que, por lo visto, este tipo de métodos de la empresa de muebles más famosa del mundo también era habitual en sus filiales de otros países.

Y, por supuesto, si el espionaje económico e industrial salpica a decenas de países en todos los continentes, España no podía ser menos. En nuestro país se han multiplicado los ciberataques con fines comerciales en los últimos años, lo cual ha puesto sobre aviso a los agentes del Centro Nacional de Inteligencia. Por ejemplo, la fábrica de Airbus Military en Sevilla fue objeto de varios intentos de espionaje cuando estaba en la recta final del montaje de su primer A400M, un avión militar que reduce a la mitad el tiempo que tarda el ejército en rotar el personal en Líbano y no necesita escalas para volar a Afganistán. El prototipo no requiere más que mil metros para aterrizar o despegar, puede hacerlo sobre pistas no preparadas, y hasta tiene la capacidad de abastecer a otros aviones en vuelo.

Se trataba de un proyecto de suma importancia en el que España trabajaba de forma conjunta con los otros seis Estados que forman el consorcio público EADS (European Aeronautic Defence and Space), lo cual mantuvo alerta al Centro Criptológico Nacional (CCN), que es la sección que vela por la seguridad de las tecnologías de la información de las administraciones públicas, y que depende del CNI.

La mayor parte de los ataques sufridos por nuestro país consisten en inserción de troyanos o *malware*, y su fin principal es el robo de información confidencial. Estos ataques son difíciles de rastrear, lo cual dificulta la identificación y procedencia de sus responsables. En cualquier caso, tal como señala el CNI, hay situaciones que despiertan sospechas de espionaje industrial. Sucede, por ejemplo, cuando alguien solicita un empleo en una empresa y a los pocos meses se le despide sin motivo aparente, después de haber tenido acceso a información valiosa. Ése es un indicio para saber que algo ha ocurrido, pero, generalmente, es demasiado tarde, ya que posiblemente el daño esté hecho. Aunque

también puede suceder al revés: una compañía le dobla el sueldo a un directivo de la competencia para ficharlo, después le saca toda la información posible de su anterior empresa y, finalmente, lo despide.

## Cuando los malos fueron los buenos

El problema de la dependencia de la tecnología es que no sólo hay que proteger los sistemas, sino estar alerta con las personas (por simple imprudencia, cualquier empleado puede convertirse en la fuente más sencilla de entrada de un ciberataque) y hasta protegerse de las mismas (en el caso de empleados desleales).

El colmo de la deslealtad ocurrió en 2002, en España. Una conocida empresa nacional, que aún hoy cotiza en bolsa —y cuyo nombre omitiré para evitar dañar su reputación, aunque haya pasado ya más de una década—, vivió una situación inesperada. Su equipo de sistemas informáticos planteó a la dirección una situación inverosímil. Sugerían una subida de sueldo en bloque a todo el departamento, como condición *sine qua non* para que los sistemas de la empresa «no dejaran de funcionar permanentemente» desde el lunes siguiente. Efectivamente, un grupo de personas, los responsables de sistemas, estaba chantajeando en bloque a su compañía, y, o les subían el sueldo de manera radical, o todo dejaría de funcionar, lo cual supondría un enorme coste en sus finanzas y su reputación. Era un chantaje en toda regla, y por parte de su propia plantilla.

Esta empresa, que es una compañía importante, tuvo que tomar una decisión traumática. O accedía a las peticiones de los chantajistas, o tardarían mucho tiempo en tener el control de los sistemas; además, la cantidad de dinero que perderían esos días sin control sería enorme, y el daño en su imagen sería inimaginable de cara a sus clientes actuales y futuros.

La solución fue salomónica. Se contrató a un grupo de hackers de una empresa de seguridad informática y se les pidió que, desde el viernes por la tarde hasta el domingo, trabajaran las veinticuatro horas del día para atacar sus propios sistemas, entrar en los mismos, robar las credenciales a los miembros de su plantilla, tomar el control y cerrarles cualquier tipo de acceso y puerta trasera que estos hubieran podido crear.

Debió de ser un fin de semana intenso. Si los hackers lo conseguían, el lunes a las 9.00 horas, a todos y cada uno de los

informáticos les esperaría la policía y un burofax con el comunicado de despido. Si no lo lograban, la única salida sería poner buena cara, tragar y plegarse a las exigencias salariales de los chantajistas; un mal menor.

Sólo diré que hubo suerte. Lo lograron. El lunes a media mañana ya ninguno de esos informáticos infieles trabajaba ya en la compañía.

Este caso nos hace ver dos cosas. La primera, cómo un pequeño grupo de personas que se pongan de acuerdo puede poner en jaque a una gran corporación, aunque sea una de las grandes petroleras o uno de los grandes bancos del mundo. La segunda, cómo un equipo bien preparado, con tecnología y el *know how* suficiente puede entrar en una empresa relevante (en este caso, una destacada compañía cotizada) y tomar el control absoluto de la misma. Hubo suerte, y los malos eran los buenos. Pero la historia podría haber pasado de otra manera bien distinta.

## El ataque que cambió tu tarjeta de crédito

En Estados Unidos, los ataques informáticos a empresas cotizadas tienen, por imperativo legal, que ser comunicados a los usuarios. Existe una cierta obligación de transparencia. Hay que dar explicaciones, y los clientes deben saber que han sido comprometidas sus cuentas, contraseñas, tarjetas de crédito, etc.

Sin embargo, en Europa, a día de hoy, no existe esta obligación legal —aunque parece que la Comisión Europea no tardará en exigirla—. Ése es uno de los motivos por los que parece que aquí no pasa nada; tal vez por eso vivimos en una especie de mundo de Yupi donde estas cosas parecen más propias de películas de ciencia ficción. Especialmente, parece que nuestros bancos sean invulnerables, mientras que, desde el otro lado del Atlántico, nos llegan frecuentes noticias de incursiones, robos, estafas, etcétera.

Aunque en Europa estos ataques se suelen ocultar, y hoy en día se esconden principalmente para no poner en riesgo la reputación y para evitar la fuga de clientes, eso no quiere decir que no ocurran y, sobre todo, que no tengan consecuencias.

Todos tenemos una tarjeta tipo VISA o Mastercard en el bolsillo. Lo que el ciudadano de a pie no sabe es que el cambio que tuvo lugar hace pocos años, deprisa y corriendo, del «plástico» que lleva en su cartera por otro se debió a un fuerte ataque informático que recibieron las redes de nuestro país, y que, por supuesto, no trascendió.

Una directiva europea obligaba a este cambio antes del fin de 2011. Las tarjetas con chip incorporado eran mucho más seguras. De hecho, el fraude con las anteriores, de banda magnética, empezaba a ser cotidiano. Para duplicarlas bastaba un lector que leyera y clonara la banda magnética y una cámara colocada en un cajero, por ejemplo, que grabara el pin del usuario. Pero, pese a la directiva europea, los distintos operadores no se ponían de acuerdo sobre el estándar a emplear. Y así pasaban los meses.

Entonces ocurrió lo inesperado. Comenzó una serie de ataques informáticos muy sofisticados, ya que actuaban sobre una norma que hasta la fecha se creía segura, la norma X.25.[1] Estos ataques

no eran cosa de cuatro o cinco chavales probando cosas, así que se alertó de inmediato a las fuerzas y cuerpos de seguridad del Estado. Se trataba de un asunto económico de vital importancia. Se estaban comprometiendo cientos de miles de tarjetas de crédito que estaban siendo robadas de forma inexplicable y muy sofisticada. Y nadie sabía cómo ni por dónde.

Por sí sola, la policía no tenía capacidad para detener estos ataques ni para identificar cómo estaban produciéndose, de modo que solicitó la ayuda de empresas especializadas. Una de ellas fue la que descubrió lo que hasta entonces no era explicable. Que los ataques ocurrían bajo la citada norma X.25.

Este hecho, y los cientos de miles, tal vez millones, de tarjetas de crédito comprometidas en España aceleraron lo que hasta la fecha se tomaba con calma. Muy posiblemente, tu tarjeta y la mía también estaban entre ellas. Para no crear alarma social, aquello se llevó con enorme discreción, y hasta la fecha jamás había trascendido.

La inmediata consecuencia fue el urgente cambio del «plástico» que llevábamos en el bolsillo todos los españoles por otro más seguro, con chip. ¿Más seguro hasta cuándo? Bueno, esperemos que dure unos años, pero lo que es inexpugnable hoy dejará de serlo poco a poco, a medida que la tecnología avance, y habrá que cambiarlo de nuevo.

La pregunta puede ser: ¿quién realizó estos ataques y logró robar una cantidad muy relevante de tarjetas de crédito de españoles? La respuesta obvia es pensar en mafias, delincuencia común, etc. Sin embargo, años después, dos personas que habían trabajado en esta operación se encontraron casualmente.

Una de ellas era uno de los policías que había trabajado en la detección de la fuga de información. La otra era uno de los empleados de la firma de seguridad que había detectado el ataque de la norma X.25, hasta ese momento inexpugnable. Al coincidir, recordaron el tema y quisieron tomar un café aparte del grupo con el que se encontraban. Con el tiempo, a ambos les había quedado un poso raro de todo aquello y querían compartirlo: «He pensado mucho... Y cuanto más lo pienso, por más que pasa el tiempo, menos me cuadra… ¿Nos utilizaron?», dijo uno de ellos.

Y es que nunca se descubrió a los culpables. Esa sospecha que tanto el policía como el informático habían compartido sin saberlo a lo largo del tiempo se formulaba en un interrogante: ¿acaso un ataque tan complejo y sofisticado no podría estar destinado a «meter miedo» para provocar el cambio al nuevo sistema con chip lo antes posible? La situación estaba estancada, ya que los diferentes operadores no se ponían de acuerdo en el sistema a utilizar, mucho dinero estaba en juego con el cambio de todos los «plásticos». Cuando se comete un delito, una norma policial básica es pensar siempre en el beneficiario de todo como sospechoso. En este caso, varias empresas se beneficiaron con contratos de millones de euros. El policía y el hacker no asegurarán que dichas empresas estuvieran implicadas, pero, sin ningún tipo de duda, en ese café ambos reconocieron estar pensando lo mismo. Su sensación era clara. Aquello no cuadraba. ¿Habían sido utilizados?

## El gran negocio del espionaje tecnológico

En ocasiones, las compañías no ejercen directamente este tipo de espionaje, sino que contratan a agencias especializadas para conseguir sus objetivos económicos. En las últimas décadas ha florecido todo un mercado de empresas que ofrecen servicios de espionaje privados a otras compañías o a gobiernos, como el ejemplo antes mencionado de Sûreté International, que trabajó para Ikea en Francia. Otra de esas empresas es Diligence, fundada por antiguos miembros de la CIA y del servicio de inteligencia británico MI5, que se presenta como una empresa especializada en investigaciones transfronterizas complejas y ofrece a sus clientes información recopilada por cualquier medio. Sí, he dicho cualquier medio.

Otro ejemplo es Aegis, una empresa que ofrece seguridad, investigaciones privadas, entrenamiento militar y servicios de consultoría, un negocio parecido al de Academi, antes conocida como Blackwater, una agencia militar privada estadounidense que presta servicios de seguridad, inteligencia y logística. Actualmente, Academi es la contratista privada más importante del Departamento de Estado de Estados Unidos, y también provee servicios a la CIA. Algunas misiones realizadas por Academi han despertado polémica debido a sus métodos poco ortodoxos. En 2007, esta empresa se vio envuelta en la muerte de diecisiete civiles durante la guerra de Irak, en el transcurso de una emboscada. El FBI determinó que catorce de los diecisiete civiles habían sido tiroteados desde vehículos de Academi (por entonces, aún llamada Blackwater), y el gobierno de Irak pidió que la compañía se retirara del país.

Pero Academi también trabaja para compañías como Deutsche Bank, Barclays o Monsanto; de esta última se rumorea que contrató sus servicios para infiltrarse en los grupos ecologistas y de defensa de los animales.

Sin embargo, quien seguramente ostenta el primer puesto por facturación y actividad en el próspero negocio de las investigaciones privadas es Kroll Inc. Tras el eufemismo de la expresión «especialización en investigaciones e inteligencia empresarial», esta

compañía estadounidense vende sus servicios de espionaje al mejor postor, y cuenta entre sus clientes con un buen número de gobiernos de diversos Estados. Su fundador, Jules B. Kroll, dice que el objetivo de su empresa es perseguir el crimen sin fronteras (especialmente el crimen financiero) cuando organizaciones como el FBI y la CIA están «muy ocupadas».

Pero lo cierto es que Kroll se ha hecho de oro trabajando para algunas de las compañías más importantes de Wall Street, así como para una larga lista de empresas, bufetes de abogados, bancos de inversión, consultoras y fondos. Le gusta decir que «la luz del sol es un maravilloso antiséptico», pero él y su compañía han sido mucho más valorados por mantener las cosas en la más completa oscuridad, actuando como guardianes de innumerables secretos embarazosos que podrían arruinar las carreras de muchos. No hay nada más rentable que conocer secretos y no divulgarlos, pero, sin embargo, poder hacerlo.

Kroll ofrece servicios de gestión de crisis o análisis de la competencia en un mundo empresarial globalizado en el que el espionaje industrial, la falsificación, el fraude informático, la suplantación de identidad y los delitos financieros sofisticados han florecido. La agencia se granjeó gran fama después de resolver algunos casos complicados para varios gobiernos de diferentes países.

Por ejemplo, a petición del gobierno de Haití, descubrió el paradero de la fortuna ilegal del dictador Jean-Claude Duvalier. También destapó, para el gobierno de Kuwait, el destino de 10.000 millones de dólares que Sadam Husein tenía depositados en bancos occidentales, y descubrió que el dictador era un gran accionista de Hachette, la primera editorial de Francia (esto no le hizo mucha gracia a los franceses). Para el gobierno de Boris Yeltsin, Kroll rastreó la enorme fuga de capitales que sufría el país, así como el elevado número de cuentas exteriores del antiguo KGB, destapando una trama de blanqueo de dinero de los antiguos servicios secretos soviéticos. Por cierto, al gobierno de Rusia tampoco le gustó lo que Kroll había averiguado, y se negó a saldar su deuda con la compañía. Otras de sus hazañas incluyen la identificación de los

tesoros ocultos de los filipinos Ferdinand e Imelda Marcos y la imputación judicial del tesorero de Fernando Collor de Mello, lo cual propiciaría la caída política del entonces presidente brasileño.

A pesar de su aparente barniz de integridad moral y profesionalidad, las actividades de Kroll, que cuenta con 3.000 empleados y presencia en 35 países, han despertado la desconfianza de muchos. Algunos acusan a la agencia de ser «una CIA privada», y de servir más a los intereses de su país, Estados Unidos, que de velar por la seguridad internacional. Cierto o no, es un dilema que tal vez sea más complejo de lo que parece a simple vista.

## El floreciente mercado de los *zero days*

Otro negocio complementario al de las empresas que ofrecen servicios de espionaje es el de las compañías que desarrollan y venden *software* espía a gobiernos y a otras empresas. Este mercado, como el anterior, vive una época floreciente desde los atentados del 11 de septiembre de 2001, y mueve cada año miles de millones de dólares. Se trata de un mundo que opera siempre entre las sombras y vive al filo de la legalidad, pero del que disponemos de un poco más de información desde que Wikileaks hiciera públicos sus Spy Files, una colección de documentos recopilada por la organización sobre este tipo de compañías. Wikileaks dispone, incluso, de un registro completo de los viajes realizados por los representantes comerciales de estas empresas, que ha elaborado su propia Unidad de Contraespionaje pinchando los teléfonos de los individuos investigados.

Gracias a esta otra labor de espionaje sabemos que un buen número de los representantes comerciales de las empresas de *software* espía más importantes del mundo han pasado por España en los últimos años. No sabemos con qué objeto vinieron a nuestro país, es posible que llegaran atraídos por el sol y las playas, pero la insistencia en los viajes y las fechas elegidas hacen sospechar que fueron más bien los negocios los que motivaron su visita. Del mismo modo, podemos pensar que, además de visitar determinadas agencias gubernamentales, aprovechaban para visitar empresas privadas.

Esta industria del espionaje pone a disposición de los gobiernos (aunque también de otras empresas) las herramientas para espiar de modo ilegítimo a los ciudadanos, amparados en una escasa vigilancia y una regulación insuficiente. Es el caso de compañías como Gamma Group, que comercializa dispositivos de espionaje diversos: desde furgonetas de vigilancia y seguimiento hasta infraestructuras para interceptar y controlar todas las comunicaciones de una red telefónica.

Sus principales clientes son las fuerzas de seguridad de una gran variedad de Estados, y su producto estrella es el FinFisher, un

*software* que permite poner bajo vigilancia a cualquier persona a través de su propio ordenador o teléfono móvil. Lo único que hace falta es que el espiado acepte con un clic la instalación de una actualización de cierto programa informático y, *voilà*, ya pueden saber todo lo que quieran sobre él. El que la víctima acepte no suele ser demasiado difícil si se le investiga bien y se conoce su actividad habitual.

No es casual que, en 2013, Gamma Group fuera incluido en la lista «Enemigos de internet», que elabora cada año Reporteros Sin Fronteras (RSF), por considerar que sus productos violan sistemáticamente los derechos humanos al facilitar la persecución de disidentes, periodistas o activistas. Por ejemplo, la compañía Gamma ha sido acusada de vender su FinFisher al Egipto de Mubarak durante la primavera árabe, así como a la familia real de Baréin (país considerado también enemigo de internet), lo cual facilitó el arresto de informadores.

La compañía, cuyos representantes visitaron España varias veces en los últimos años, aparecía en el informe «Enemigos de internet de RSF» junto al de varios países que no respetan la libertad de prensa y al de otras cuatro empresas a las que se acusaba de actividades similares a las de Gamma. Estas empresas son Trovicor, Amesys, Hacking Team y Blue Coat.

Trovicor es uno de los proveedores más importantes de soluciones legales de interceptación de contenidos en el mundo. En 2010, esta sociedad limitada fue interrogada en una audiencia en el Parlamento Europeo por suministrar su tecnología a los regímenes de Irán, Baréin y Siria, que después la emplean para perseguir, encarcelar y torturar a periodistas.

Amesys, una empresa de capital francés, desarrolló un *software* llamado Eagle que después vendió a varios países, entre ellos la Libia de la que todavía era dictador Gadafi. Posteriormente, el régimen libio empleó esa tecnología para vigilar a periodistas y activistas de derechos humanos, motivo por el que la empresa ha sido llevada ante la justicia francesa por la Federación Internacional de Derechos Humanos (FIDH), que la acusó de complicidad en las torturas.

Hacking Team es una empresa italiana que describe sus propias tecnologías como «ofensivas», y ha sido cuestionada por la venta de sus productos a Marruecos y a Emiratos Árabes Unidos. El Remote Control System (RCS) que han desarrollado, y que han bautizado con extrema modestia como «Da Vinci» y «Galileo», es capaz de romper el cifrado utilizado por correos electrónicos, archivos y protocolos VOIP. El RCS permite también interceptar los datos de los navegadores, de aplicaciones como Skype y de redes sociales como Facebook, así como los correos electrónicos, la localización y las llamadas telefónicas del sujeto que ha sido puesto bajo vigilancia.

Por último, Blue Coat es una empresa de Silicon Valley especializada en tecnologías de la información, y cuya mala fama se debe sobre todo a haber proporcionado herramientas de filtrado y censura a países tan amantes de las libertades y contrarios a todo tipo de abuso como Siria o Myanmar. Angelitos.

Pero estas empresas representan sólo un puñado de las muchas que han hecho fortuna en el negocio del *software* espía. Hay muchas más y, algunas, como Telesoft Technologies, Utimaco, Rohde & Schwarz, Verint Solutions o Hidden Technology, han estado en nuestro país últimamente. Quizá haciendo turismo. Quizá haciendo negocios. Tal vez ambas.

Por supuesto, como sucede con la droga, para que haya camellos y producto, debe haber consumidores. Es más que evidente que hay empresas —¡y gobiernos, muchos gobiernos!— que están interesadas en estas soluciones en nuestro país. De hecho, muchas de ellas ya las han probado y adquirido.

## El cazador cazado

Fue un día tonto de julio de 2015 cuando ocurrió algo sorprendente. Nuestros amigos italianos, los «enemigos de internet», los expertos hackers contratados por gobiernos de todo el mundo tenían un serio problema.

Se filtraron en la red miles de archivos y correos electrónicos de Hacking Team. Alguien había hackeado todos sus sistemas, dejando al descubierto toda la información de la compañía, desde miles de correos electrónicos hasta facturas, documentación interna, claves de sus programas, contactos comerciales y *software* con sus *exploits* y su código fuente.

Todo había quedado volcado en internet para quien quisiera acceder a ello. Hasta 400 GB de información de todo tipo que hoy pueden leerse en varias páginas, entre ellas, Wikileaks.

Esto ha hecho que lo sepamos absolutamente todo sobre la firma y sus actividades. Por ejemplo, el país que más dinero gastó en programas espía, virus y *malware* es México. Agencias como el FBI, los servicios de inteligencia rusos o el CNI español eran clientes activos en el momento de la filtración, y pagaban religiosamente sus licencias a precios variables según mercado. Había hasta 97 clientes de 35 países, incluyendo (aunque la firma lo había negado en público en varias ocasiones) países de regímenes autoritarios como Sudán, que desde luego han debido hacer un uso poco ético del *software*. Este país en concreto tenía un contrato de un millón de dólares y había depositado ya un pago de 500.000 dólares, según la información que hoy conocemos.

De Etiopía se sospechaba que había utilizado los servicios de Hacking Team para espiar a los periodistas de Ethiopian Satellite Television; hoy sabemos que eso no era una sospecha, sino que está confirmado.

Los angelitos de Hacking Team incluso intentaron vender al Estado del Ciudad del Vaticano sus virus y troyanos sin rubor. Desde luego eran temerarios, y, tras todo esto, no creo que puedan ir al cielo. Hasta preparaban una aplicación de móvil con el señuelo de la Biblia para poder infectar terminales.

Entre los miles de correos electrónicos, los hay de la policía española, que negociaba con los italianos por medio de una empresa intermediaria con sede en Madrid. Incluso hay correos electrónicos en los que los policías solicitan ayuda para infectar terminales de usuarios, reciben instrucciones y confirman que han podido hacerlo «al primer intento con éxito».

Es preocupante ver que la policía (aunque su contrato no parecía activo ya en el momento del hackeo) y el CNI español eran clientes de dicha firma. Es decir, que pagaban por virus y *exploits* con los que intuyo que algo harían… Si se han utilizado sin que lo autorizara un juez, se habría estado vulnerando el artículo 18.3 de la Constitución respecto a la privacidad de las comunicaciones. Si alguien de la esfera política tira «en serio» del hilo, me temo que aquí va a haber sorpresas, y que los mandos del CNI se van a ver en un problema.

Hasta la fecha, en España no hay ley alguna que habilite a los cuerpos y las fuerzas de seguridad del Estado para utilizar virus o troyanos contra los usuarios. Me dicen que es posible que esa ley se apruebe en breve, como en Alemania, pero, desde luego, eso aún no ha ocurrido. Hacking Team ponía a disposición del CNI un portal para que generaran sus propios programas de *malware* basados en vulnerabilidades *zerodays*. Ya están tardando algunos partidos políticos, esos que son tan rápidos para otras tonterías, en preguntar en el Parlamento español contra quién se han utilizado estas herramientas y en confirmar si había orden judicial previa. No es por ser mal pensado, pero uno no suele pedir permiso para utilizar una herramienta que oficialmente no tienes y no existe. Asunto complicado.

En algunos correos electrónicos se lee cómo algunos responsables del CNI piden ayuda a la empresa de *hacking* italiana, ya que habían tenido un problema de seguridad y alguien había «hackeado sus *proxies*». Eso no deja en buen lugar a nuestras élites de inteligencia, y nos hace reflexionar sobre en qué manos estamos…

Otra cosa curiosa que hemos podido descubrir es cómo el FBI utilizaba el *software* de los italianos para desenmascarar a usuarios

que usan la red TOR. Primero los infectaba, y luego revelaba su IP real cuando estuvieran usando TOR. El FBI gastó hasta 775.000 dólares en el uso de herramientas de Hacking Team.

En general, este escándalo, del que sabremos mucho más en los próximos meses (a medida que se vayan leyendo los cientos de miles de correos electrónicos filtrados), era previsible y no ofrece muchas sorpresas sobre lo que los malpensados teníamos en mente que estaba sucediendo… Bueno, sí, ¡ofrece una sorpresa!

La realidad siempre supera la ficción. Una de las funcionalidades del *software* denominado RCS era insertar en el ordenador de la víctima contenidos incriminatorios; en concreto, archivos pornográficos y pedófilos, así como documentos sobre cómo elaborar bombas. Es decir, una de las funcionalidades de unos programas que se vendían sólo a agencias gubernamentales era permitir introducir en el ordenador de la víctima archivos que pudieran resultar incriminatorios para, posteriormente, justificar una detención. Es evidente que si ésa era una funcionalidad del *software* sería porque sus clientes (las agencias gubernamentales) lo habían demandado. Es decir, entiendo que consideraran «normal» pagar cientos de miles de dólares por programas que entraban en dispositivos de la gente y les podían dejar instalados vídeos pedófilos o contenidos proterroristas. Me parece de una gravedad extrema.

Por cierto, como conclusión final de todo este incidente hemos aprendido otras lecciones valiosas… Los italianos tenían *exploits* para entrar como Pedro por su casa en ordenadores y móviles Android (especialmente si tenían permisos *root*) y iPhone (en caso de tener *jailbreak).* En el caso contrario era mucho más complicado, y podían llegar a necesitar acceso físico al terminal.

Eso sí, la principal conclusión es que uno de los mayores coladeros son las vulnerabilidades de Abode Flash Player en tu navegador, ya sea Internet Explorer, Chrome, Safari o Firefox. Estos agujeros de seguridad permiten que, simplemente visitando una web y sin que te enteres, alguien te introduzca sin ningún problema un código malicioso en tu ordenador. Incluso días después de la filtración, algunas de estas vulnerabilidades seguían sin ser solucionadas por parte del fabricante. Dado que tener Flash no es

imprescindible ya para navegar por internet, es recomendable desinstalarlo. En internet encontrarás decenas de artículos que, tras este incidente, lo recomiendan y explican cómo hacerlo.

Una cosa más…, como curiosidad. Comprometer 400 GB de información es algo muy complicado de hacer entrando remotamente en servidores de internet; la brecha tendría que haber sido enorme y haber durado mucho tiempo. Hay quien piensa que fue un acceso físico a los servidores de Hacking Team, y que alguien copió los discos duros.

Se puede perder la fe y la reputación. El que pierde de esta manera la reputación en internet no la recupera nunca. Esta empresa ha dejado en evidencia a gobiernos y empresas de todo el mundo. Sus claves, sus contactos, personas que trabajan en ellas, su negocio y sus actividades.

El cazador ha sido cazado. Y tal vez lo merecía.

## Silicon Valley, la sede de esos brillantes muchachos que trabajan para la NSA

A pesar de que existe un próspero mercado de empresas de espionaje y *software* de vigilancia, en muchas ocasiones los Estados no necesitan recurrir a ellas. Pueden obtener ellos mismos la información que desean con la ayuda de las multinacionales de las telecomunicaciones. En Estados Unidos, el patriotismo se vive de forma distinta (y, a menudo, más intensa) que en Europa, por lo que no es de extrañar que muchas empresas norteamericanas colaboren de buen grado con su Gobierno e identifiquen los intereses económicos de Estados Unidos con cuestiones de seguridad nacional. Esto hace que, frecuentemente, las compañías estadounidenses se comporten como verdaderos apéndices de la política de la Casa Blanca, hasta el punto de que los propios trabajadores de estas compañías son incapaces de discernir si están trabajando para su empresa o para el Gobierno.

Un buen ejemplo para ilustrar el grado de implicación y coordinación de las empresas estadounidenses con su gobierno es la compra de Skype por Microsoft en 2011. El gigante de Bill Gates adquirió la compañía danesa en una operación que siempre ha estado rodeada de polémica. Curiosamente, dicha compra fue cara, y la incorporación de Skype no ha dado grandes beneficios a Microsoft. Sin embargo, era sabido que la NSA estaba tratando de descifrar sin éxito las comunicaciones de la empresa. Después de conseguir tener acceso a las llamadas de voz y los correos electrónicos de los ciudadanos, las videollamadas eran la última pieza en el espionaje global y total al que aspira la agencia de seguridad estadounidense, pero el sistema de encriptación de Skype se les resistía.

La realidad es que desde que Microsoft adquirió Skype, la compañía de Bill Gates ha estado ayudando a la NSA para que las comunicaciones de los usuarios sean interceptadas por el sistema de vigilancia PRISM. El hecho de que la compra de Skype fuese una operación económica «extraña», unido a las revelaciones posteriores, han llevado a algunos a pensar que fue el propio

Gobierno estadounidense el que solicitó a Bill Gates que se hiciera con Skype para facilitarle su objetivo de interceptar todas las comunicaciones. Y si no fue realmente así, podemos afirmar categóricamente que el segundo gran beneficiario de esta operación, más allá de los fundadores de Skype, que se llevaron lo suyo, fueron las agencias gubernamentales norteamericanas, especialmente la propia NSA. A los accionistas de Microsoft posiblemente les importe haberse pulido absurdamente y de una tacada 5.920 milloncejos de euros de nada. El beneficio de la empresa compradora, con Bill Gates a la cabeza, está aún por dilucidar. En este punto, su papel es poco más que el de «pagafantas» de esta película.

Por supuesto, éste no ha sido el caso único en el que la empresa de Redmond ha «ayudado» en sus problemillas de encriptación al Gobierno de Estados Unidos. Sin ir más lejos, Microsoft colaboró con la agencia de seguridad estadounidense para que el Gobierno pudiera eludir el sistema de encriptado que protege las conversaciones entre usuarios de su mensajería electrónica Outlook. ¡Ojo! En Microsoft no son unos esquiroles, ni se comportan de manera agresiva con nosotros; no son ni mejores ni peores que Google, Twitter, Facebook, Yahoo! o Instagram. Son, simplemente, parte del sistema de sumisión de las grandes tecnológicas norteamericanas a su propio Gobierno.

Multinacionales como Google, Facebook, Dropbox, Apple, AOL o Yahoo! también aparecen como empresas que suministran información al Gobierno de Estados Unidos. Aunque ya nadie las cree, reiteradamente han tratado de negar estos hechos, asegurando que sus sistemas no contienen «puertas traseras» para facilitar el acceso a la información privada de sus servidores. Las evidencias hacen cada vez menos convincentes sus argumentos.

Por ejemplo, cuando el presidente ejecutivo de Google, Eric Schmidt, afirmó en una entrevista con *The Wall Street Journal* que el Gobierno de Estados Unidos había accedido sin autorización a la información de sus servidores, calificó como «indignante» la actuación de la NSA. Sin embargo, los documentos aportados por Snowden demostraron que las empresas mentían, y, ante la evidencia, las compañías tuvieron que admitir que sí suministraban

información privada a la NSA, pero trataron de justificarse alegando que lo hacían por imperativo legal.

En la mayoría de los casos, la multinacionales colaboran de buen grado con la NSA, facilitándole un acceso permanente y sin autorización previa a toda la información privada almacenada en sus servidores. Además, según desveló el diario *The Guardian*, la NSA paga millones de dólares a las multinacionales tecnológicas para asegurarse su complicidad en el proceso de vigilancia. En cualquier caso, si el patriotismo y el dinero no son suficientes para promover la colaboración de las empresas estadounidenses, el Gobierno del país dispone de la Ley Patriótica, que fue aprobada tras los atentados del 11 de septiembre de 2001, y que amplió los poderes de vigilancia contra los delitos de terrorismo. Es decir, esto puede hacerse por las buenas… o por las malas, y, en principio, la predisposición de los gerifaltes de las grandes compañías es la de ofrecer silencio, abrazos y máxima colaboración.

Amparado en esta ley, el Gobierno de Estados Unidos ha ejercido un espionaje masivo, tanto sobre extranjeros como sobre sus propios ciudadanos. La NSA siempre ha negado este último extremo, asegurando que no se había puesto bajo vigilancia a ningún individuo norteamericano que no fuera sospechoso de estar involucrado en actividades delictivas, y que todos los objetivos de vigilancia son extranjeros y residentes fuera del país. El tiempo y la documentación filtrada ha demostrado que la NSA miente, y que también los ciudadanos estadounidenses han sido espiados masivamente. Pero, en cualquier caso, no dejan de ser llamativas las explicaciones de la agencia: ¿te imaginas al presidente del Gobierno de España asegurando en rueda de prensa que el CNI no espía a los españoles, que sólo tiene bajo vigilancia a marroquíes y rumanos? La fiesta que se iba a liar sería épica. A mucha gente le parecería intolerable e incluso xenófobo. Pero claro, estamos en Europa, y la exigencia en cuestiones morales y de privacidad no es la misma que en los Estados Unidos de América, donde esa explicación (que podríamos caricaturizar como «violamos los derechos de los otros, no los tuyos, que eres de los nuestros») está aceptada por el 90 por

ciento de los ciudadanos. Solamente algunos pequeños grupos de activistas se llevan las manos a la cabeza.

Nacionales o extranjeros, lo cierto es que, desde el 11 de septiembre de 2001, se ha producido un giro en las políticas de vigilancia sobre los ciudadanos. Por un lado, las amenazas contra la seguridad del mundo contemporáneo provienen de grupos e individuos más que de Estados, lo cual obliga a que el objetivo de la vigilancia sea más el público que los gobiernos. Además, puesto que el tráfico de los usuarios viaja e interacciona con el tráfico de otros usuarios, poner bajo vigilancia a un ciudadano hace posible el acceso a los datos de otros individuos al mismo tiempo. Por último, más allá de las legislaciones, el desarrollo tecnológico de los servicios de inteligencia estadounidenses están varios años (se dice que entre cinco y diez) por delante de la tecnología de que disponen los ciudadanos y otros gobiernos, lo cual les permite acceder a prácticamente cualquier información privada sin que los espiados puedan saberlo y, por tanto, sin que el Gobierno rinda cuentas por ello.

## Así leen los amigos de la NSA tu correo electrónico

Pero ¿de qué modo lleva a cabo exactamente la NSA su espionaje sobre los ciudadanos? ¿Cómo accede el Gobierno de Estados Unidos a nuestro Facebook o a nuestro correo de Gmail? Y la pregunta del millón: ¿es legal?

En determinados países como China, Corea del Norte, Siria o Irán, es una obviedad decir que hay una total barra libre. Eso lo esperabas, como es evidente, pero seguro que esperas algo más de vergüenza torera en las democracias del mundo y los países de nuestro entorno.

Para los servicios secretos de los países occidentales, la legalidad es relativa. No llega a representar ni tan siquiera una traba burocrática para sus actividades. Lo más que pudiera ocurrir es que, si hay algún exceso, se tengan que forzar un par de dimisiones, retiros forzados, abrazos, medallas a los servicios prestados, entregadas en privado y jubilaciones prematuras. Poco más. La ley no importa. Todo vale y, si no fuera así, se creará una ley a medida para que así sea.

Vamos, que en un ranking de trasparencia, protección y respeto a las libertades por parte de los servicios secretos, nuestra sociedad no está tan alejada de los países del primer grupo como cabría suponer.

La Cuarta Enmienda de la Constitución estadounidense establece que «el derecho de los habitantes a la seguridad en sus personas, domicilios, papeles y efectos, contra incautaciones y pesquisas arbitrarias, será inviolable, y no se expedirán órdenes al efecto, a menos que exista una causa probable, corroborada mediante juramento o declaración solemne, y cuyo contenido describa con exactitud el lugar a ser registrado y las personas o cosas que serán objeto de detención o embargo». Es decir, que la Cuarta Enmienda dicta que el Gobierno necesita una orden judicial para investigar a un ciudadano estadounidense. ¡Ah, espera!, si no tienes la nacionalidad estadounidense no estás protegido por esta enmienda constitucional, chico, ¡mala suerte! Ésta es una manera de dividir a la población entre ciudadanos de primera (los nuestros) y

ciudadanos de segunda (todos los demás), autorizando a los de primera a violar cualquier derecho moral y legal que los de segunda puedan poseer.

Aunque la ley les sirve de coartada, no nos engañemos, tampoco es que la necesiten demasiado. En realidad, conseguir una orden judicial no es muy complicado para la NSA, que puede obtenerla rápidamente a través de un tribunal secreto llamado Foreign Intelligence Surveillance Court (FISC), algo así como Tribunal de Vigilancia de Inteligencia Extranjera. Esta corte tiene la particularidad de que sólo admite al abogado que representa al Gobierno y nunca hace públicas sus sentencias ni decisiones. Y, a pesar de todo ello, es legal. Un ejemplo de trasparencia democrática que hace, entre otras muchas cosas, que con el señuelo del terrorismo sean espiadas relaciones personales, líderes mundiales, personas anónimas, altos directivos, empresarios e incluso ONG de forma masiva y sin control alguno.

De las 1.800 órdenes de investigación que el FBI y la NSA solicitaron en 2012, el 98,9 por ciento fueron aprobadas por ese tribunal. ¡Qué efectividad, chicos! Y, una vez se han hecho con la orden judicial, las empresas están obligadas por ley a suministrar al Gobierno la información que solicite. Me encantaría haber podido tener acceso al 1,1 por ciento restante, pero no ha sido posible. Imagino que serán defectos de forma, o una manera de que no se pueda decir que el tribunal es un pasteleo total.

Pero pensarás, y con razón, que esas 1.800 órdenes no se corresponden con el espionaje masivo que han destapado los papeles de Snowden, y que es imposible que el Gobierno de Estados Unidos haya solicitado y conseguido una orden judicial para investigar a millones de ciudadanos. Efectivamente, la NSA espía a ciudadanos propios y extraños de forma completamente ilegal con la necesaria colaboración de las empresas operadoras de internet.

Pero, tal como advirtió Alberto Sicilia en el diario *Público*, para entender mejor cómo se lleva a cabo el espionaje es interesante analizar las palabras de un antiguo portavoz de Facebook, conocedor, por motivos obvios, de la causa: «Cuando el Gobierno pide a Facebook datos sobre individuos, nosotros sólo entregamos

los estrictamente requeridos por la ley. Nunca permitimos un acceso directo a nuestros servidores».

Dos trucos, uno por cada frase.

El primero: «Estrictamente requeridos por la ley». Ya hemos visto que la ley les ampara en casi todo, ya que el tribunal desarrollado para ello les concede todos los privilegios, y, si eso falla, siempre pueden hacerlo mentando la amenaza terrorista.

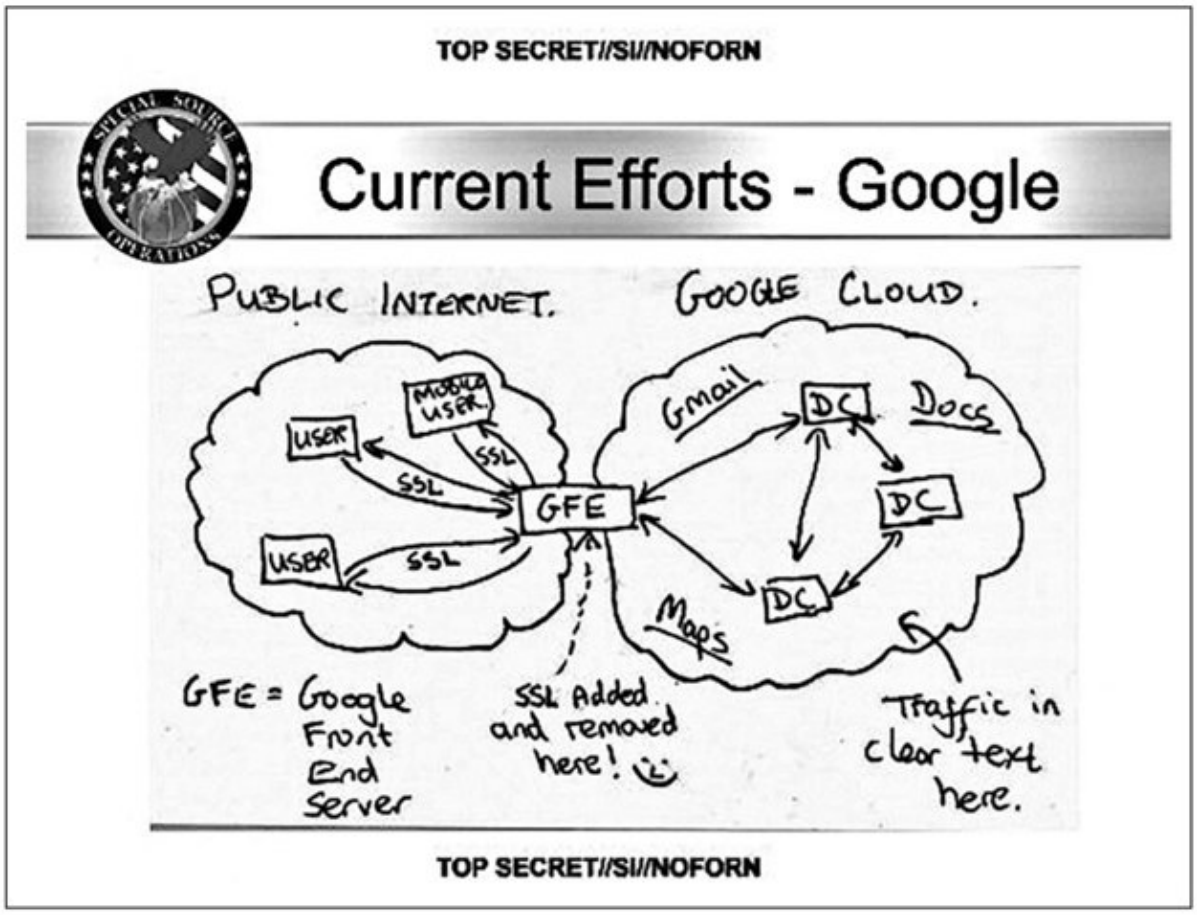
Si prestamos atención a la última frase, descubriremos el segundo truco. Se trata de una trampa lingüística. En efecto, las compañías «no permitían un acceso directo» a sus servidores. Eran un poco más sutiles: lo que hacían era copiar datos de sus servidores a otros servidores (que técnicamente no eran suyos aunque estuviesen dentro de sus instalaciones) a los que sí tenía acceso la NSA.

La operación para acceder al correo electrónico de los ciudadanos tampoco es muy complicada. Es posible que te hayas fijado en que, cuando te conectas a tu cuenta de Gmail, en la URL del navegador aparece «https://» en lugar de «http://» (la diferencia es la letra «s»). Básicamente, lo que la «s» quiere decir es que la conexión entre nuestro ordenador y el servidor de Google está encriptada con el protocolo de seguridad SSL/TLS, o sea, que es segura, de tal modo que nadie puede leer nuestros correos aunque pinchase el cable por el que viaja el mensaje desde nuestro ordenador hasta Google.

Sin embargo, Google no cuenta con un único servidor. Esto significa que, cuando nos conectamos con alguno de sus servicios, en realidad nos estamos conectando al servidor que hace de «puerta de entrada» a los sistemas de Google. Esa conexión entre nuestro ordenador y la puerta de entrada es segura. Pero, una vez nuestro correo electrónico llega a Google, la multinacional lo copia en múltiples servidores, de tal modo que, si se cayera uno de sus centros de datos, nosotros podríamos continuar navegando por Gmail sin problema.

Lo malo es que las conexiones entre los centros de datos de Google, esto es, las que se producen una vez hemos traspasado la puerta de entrada, no están encriptadas. Lo que hace la NSA, a

través de su programa MUSCULAR, es pinchar precisamente esos cables entre los centros de datos de Google (pero también de Yahoo!, por ejemplo) para poder leer los correos electrónicos. Es decir, aunque pudiera robarse nuestra información camino del centro de proceso de datos (o *data center*) de Google, habría que desencriptarla. No es imposible, pero es mucho más trabajoso que hacerlo directamente en los sistemas de Google, donde esta información no está encriptada. Para entenderlo mejor, veamos el siguiente documento gráfico que explica el proceso.




Fuente: *The Washington Post*; documentos de Snowden.

En la nube de la izquierda están dibujadas las conexiones entre los usuarios y la puerta de entrada de Google. Como puedes ver, las

flechas que indican el tráfico llevan aparejado el rótulo «SSL», lo que indica que las conexiones son seguras.

En la nube de la derecha están las conexiones internas entre los servidores de Google. Ahí ya no aparece escrito el rótulo «SSL». Es decir, las conexiones aquí no son seguras.

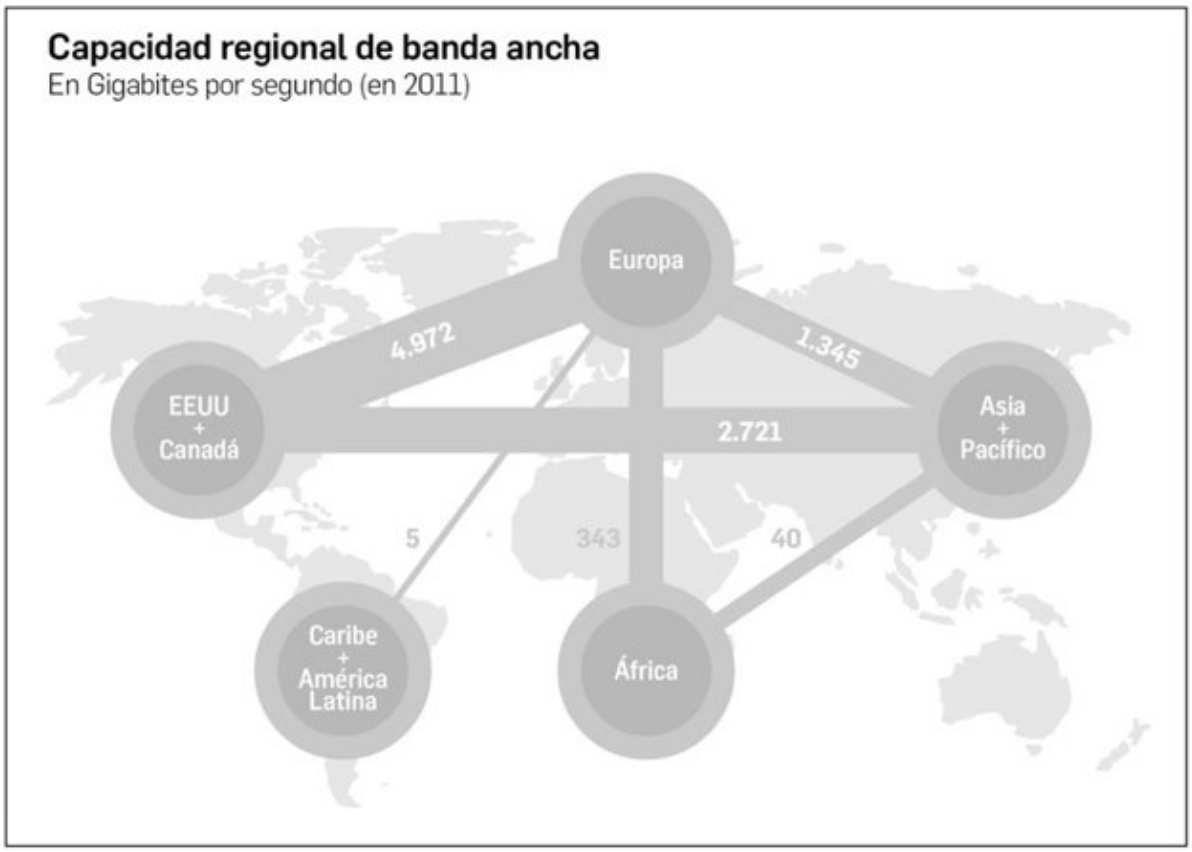
Entre las dos nubes aparece un cuadro con las siglas «GFE», la puerta de entrada a Google. Aquí está indicado que el protocolo de seguridad «SSL» desaparece una vez entras en Google. (La cara sonriente que lo acompaña no tiene desperdicio.)

Google cuenta con cientos de *data centers* (DC) repartidos por todo el mundo, muchos de los cuales están conectados por fibra óptica propia. Así, la NSA sólo tiene que pinchar estos cables para poder acceder a todos los datos que circulan sin encriptar.

Pero si Google colabora felizmente con las agencias gubernamentales estadounidenses, ¿por qué motivo la NSA estaría interesada en pincharles sus sistemas y robarles información? La respuesta es simple, porque son capaces de hacerlo, así no dependen de la colaboración bienintencionada de la empresa…, y tampoco tienen que dar explicaciones de sus prácticas, por ejemplo, si están obteniendo información y archivos de ciudadanos estadounidenses, algo vetado por la Constitución del país.

Por si fuera poco, se da la circunstancia de que, por su estatus económico y tecnológico, la mayor parte de las comunicaciones mundiales pasa por Estados Unidos, lo cual les facilita mucho las cosas. Digamos que eso convierte las redes norteamericanas en el Disneylandia de los *voyeurs.*

Esto sucede porque las llamadas telefónicas, los correos electrónicos o los chats no viajan hasta su destinatario siguiendo el camino más corto, sino el más barato, que coincide, generalmente, con el canal con mayor ancho de banda disponible. Puesto que el ancho de banda que une Norteamérica con Europa, la región Asia-Pacífico o América Latina es mayor que la de cualquiera de las combinaciones posibles entre estas tres, es probable que, por ejemplo, un correo electrónico enviado desde Francia y recibido en Brasil haya pasado antes por Estados Unidos. En el siguiente gráfico puedes ver esto que acabamos de explicar.




Fuente: *El País*.

Esta superioridad tecnológica, unida a la inmunidad de la que disfruta, es la que le ha permitido a Estados Unidos (y, en menor medida, a muchos otros Estados con un desarrollo técnico suficiente) ampliar el objeto de su vigilancia, justificando como políticas de seguridad o antiterroristas actividades eminentemente económicas. No es de extrañar que, según un informe de Verizon, Kaspersky y McAfee, el 87 por ciento de los ciberataques provenga de los gobiernos de distintos países del mundo, y que, de ellos, un alto porcentaje tengan como objetivo empresas e industrias.

## Nadie le regala a Obama un iPhone por Navidad

En cualquier caso, una vez que uno se pone a bucear en el fangoso mundo del espionaje económico e industrial, no tarda demasiado en llegar a la conclusión de que, tras la apariencia de calma y *fair play* comercial, se esconde una lucha feroz entre Estados y compañías en la que nadie queda al margen y ningún dispositivo es inofensivo. Ninguna actividad cotidiana, ni siquiera jugar a Angry Birds con nuestro iPhone, está a salvo del riesgo. Y esto no es una forma de hablar.

La estadounidense NSA y la británica GCHQ espiaron información y datos personales de millones de usuarios a través de aplicaciones gratuitas como Angry Birds. En el mundo del marketing hay una premisa que casi nunca falla: si es gratis, entonces el producto eres tú. Lo que si sé es que el presidente de Estados Unidos no juega a Angry Birds desde su iPhone, ya que tiene prohibido por sus servicios secretos utilizar este tipo de teléfono móvil. ¿El motivo? ¡Tachán! Razones de seguridad, según él mismo manifestó en el año 2013, durante una reunión con jóvenes para tratar temas de la ley sanitaria que promulgaba. Curiosamente, aunque parece haber razones de peso para que los servicios secretos no permitan usar un iPhone a su presidente, si le está permitido utilizar un iPad.

En el mundo de la seguridad también hay una premisa: si es un *smartphone*, entonces no es un teléfono, es un dispositivo de seguimiento. A través de él es sencillo geolocalizarte con gran precisión. A Obama, sin embargo, sí se le permite usar BlackBerry (que cuenta con dispositivos de encriptación más seguros que Apple y Android), aunque bajo estrictas medidas de seguridad, que incluyen un correo electrónico personal al que sólo tienen acceso diez personas. Y no puede quejarse: los anteriores presidentes de Estados Unidos ni siquiera utilizaron correo electrónico en sus mandatos, no se lo permitían los servicios de seguridad.

En España —siempre a la última moda—, el Estado hace entrega de un iPad y un iPhone como herramientas de trabajo a todos los diputados, senadores y altos cargos, incluyendo al presidente del Gobierno. Entre otras razones, tal vez esto explique por qué jugamos

en «segunda división» como país. Y, seguramente, debería darnos algo que pensar. A estas alturas ya sabes que todo lo que pase en estos aparatos de nuestra supuesta —ya, ya sé que es un término discutible— élite política, puede ser impreso, leído y compartido después, entre risas y palomitas, por un grupo de animados *yankees* en una sala oscura de un pueblecito de Wisconsin.

¡Qué barbaridad! ¿Insinúa el autor que los aparatos norteamericanos que hemos puesto en manos de nuestros dirigentes no son seguros?

No. No lo insinúo yo. Como ya has visto, lo dicen claramente los servicios secretos estadounidenses, que, pese a ser los dueños de la pelota, comprenden los riesgos que tiene y no dejan que su presidente juegue con ella ni por asomo.

Seguro que, cuando este libro vea la luz, algún carguillo de medio pelo tranquilizará a las masas sobre este supuesto, explicándonos ex cátedra que son aparatos perfectamente controlados, que de su seguridad se ocupa el mismísimo CNI y que no hay motivo de preocupación. Cuando esto ocurra, mírale a la cara. Tú conoces la realidad. Simplemente, trata de averiguar su motivación. Hay dos opciones. O es un imbécil o un inconsciente.

3

# Cibercrimen

El crimen ha acompañado a los hombres desde que pueden llamarse seres humanos. Los periódicos están llenos de crímenes cada día, así como el cine, los libros, las series de televisión, etc. Estaba aquella famosa serie protagonizada por Angela Lansbury, titulada *Se ha escrito un crimen*, y aquel diario, *El Caso*, que recogía decenas de ellos. Recuerdo el famoso crimen del expreso de Andalucía, y ese disco de Supertramp, *Crime of the century.* En la gran pantalla hemos visto *El crimen perfecto*, de Hitchcock, y muchos, bueno, está bien, unos pocos habrán leído las páginas de *Crimen y castigo*, de Dostoievski.

## ¿Qué demonios es eso del cibercrimen?

Todo el mundo sabe lo que es un crimen. Pero ¿qué es el cibercrimen? Podemos decir que el cibercrimen consiste en el uso de herramientas digitales para cometer algún tipo de actividad ilegal. El problema es que, a medida que las tecnologías de la comunicación evolucionan y se hacen más presentes en la vida de los ciudadanos, cada vez es más difícil encontrar crímenes que no impliquen, de algún modo, un componente digital. Diferenciar claramente ambos tipos de delitos puede parecer un debate estéril, pero, para la Comisión Europea, la distinción entre crímenes tradicionales y digitales no es baladí, ya que es necesario que quede reflejada y definida en las leyes de la Unión Europea. Así, la diferencia entre los cibercrímenes propiamente dichos y los crímenes tradicionales que conllevan el uso de herramientas digitales radica, según la Comisión, en que los primeros constituyen ataques que emplean exclusivamente redes digitales, tanto en sus medios como en sus fines.

Esto nos lleva a un segundo dilema. Del mismo modo que ocurre con el crimen, todo el mundo sabe lo que es un ataque. Sí. Pero ¿qué es un ciberataque? Lo cierto es que el término está rodeado de ambigüedad, porque ha sido empleado para describir desde protestas online hasta sabotajes de investigaciones nucleares, pasando por el robo de secretos en internet o actos de guerra. Como en el caso del cibercrimen, la definición de ciberataque no es una cuestión banal, especialmente si tenemos en cuenta que su número no para de crecer de forma exponencial cada año. Desde 2009, el Gobierno de Estados Unidos define un ciberataque como «una acción deliberada para alterar, interrumpir, engañar, degradar, o destruir sistemas informáticos o redes de información y/o programas alojados o en tránsito por esos sistemas o redes».

Como en el caso de los cibercrímenes y los crímenes tradicionales, los ciberataques se diferencian de los ataques convencionales en sus medios y sus fines. En lugar de emplear herramientas cinéticas (por ejemplo, el puño, una bomba o una espada), un ciberataque utiliza herramientas digitales (básicamente,

ordenadores y otros dispositivos inteligentes). Esto hace que sea mucho más versátil que un ataque tradicional, porque no está sujeto ni constreñido por las leyes de la física. Tal como señalan Peter W. Singer y Allan Friedman en su libro *Cybersecurity and cyberwar,* un ciberataque se mueve, literalmente, a la velocidad de la luz y no se detiene ante fronteras físicas o políticas. Además, sin ser divino, es ubicuo: puede tener lugar en varios lugares al mismo tiempo.

Atendiendo a su objetivo, un ciberataque siempre golpea primero un sistema informático, en lugar de un blanco físico. Es posible que de ese golpe se derive un daño físico para alguien o para algo, pero el primer impacto siempre es sobre un ordenador.

Al mismo tiempo, un ciberataque es mucho más difícil de identificar y atribuir que un ataque convencional. En muchas ocasiones, sólo se puede tener la sospecha de que el ciberataque se ha iniciado en un determinado país, pero resulta muy complicado asegurar quién es el responsable. Es lo que ocurre, por ejemplo, con un gran número de ciberataques originados en Asia. Muchas veces se sospecha que es China su lugar de procedencia, pero es prácticamente imposible probarlo, así como determinar qué actor lo ha ordenado, es decir, si se trata de empresarios, funcionarios del Gobierno, hackers o activistas.

Asimismo, predecir el efecto que tendrá un ciberataque es también más complicado. Resulta relativamente sencillo anticipar el coste en daños físicos o económicos que tendrá la detonación de una bomba en un centro comercial la víspera de Reyes, por ejemplo. Sin embargo, no es tan fácil calcular el impacto que puede tener un virus informático, ni sus consecuencias, ni su capacidad de propagación.

Como vemos, un ciberataque es bastante distinto de un ataque tradicional en sus fines y en sus medios. Pero, incluso dentro de los ciberataques encontramos distintos tipos. Los «ataques de disponibilidad» tratan de impedir el acceso a una determinada red, bien sobrecargándola de visitas, bien mediante la denegación del servicio, bien tirando abajo la página. Es el caso de los conocidos ataques DDoS, que afectan a una red causando que un servicio o recurso sea inaccesible a los usuarios legítimos.

Otro tipo son los «ataques de confidencialidad», que buscan penetrar en ciertas redes para extraer información privada y datos de los usuarios. Un ejemplo de este tipo de ciberataque es el fraude asociado a las tarjetas de crédito o las cuentas bancarias online. Los atacantes obtienen contraseñas y otras informaciones a través de ataques informáticos, o bien engañan directamente a los clientes, haciéndose pasar por una institución financiera, en una práctica muy extendida y conocida como *phishing*.

Por último, hay un tipo de ciberataque que no busca robar o extraer información, sino cambiarla. Puede constituir un simple acto de protesta o vandalismo, pero también puede tratarse de un sabotaje con graves consecuencias. Por ejemplo, ¿qué ocurriría si unos cibercriminales alteraran la información de una central nuclear o de un servicio básico para los ciudadanos, como el sistema eléctrico de un hospital? Pero de esto hablaremos un poco más adelante, cuando abordemos el problema del ciberterrorismo.

A partir de estas diferentes modalidades de ataques, los cibercriminales han desarrollado con gran imaginación algunos robos verdaderamente originales y lucrativos. Una de las ventajas que tiene el robo en internet es que no tiene por qué limitarse a un individuo solamente: ¿por qué robar a una persona cuando puedes robar a cien millones o más? Esto es lo que permiten algunos kits de ciberdelincuencia como Blackhole o SpyEye, que minimizan el coste de los robos en términos tanto económicos como humanos y permiten robar a millones de personas en pequeñas cantidades, de modo que las víctimas nunca informan del abuso a las autoridades y el delito no puede ser rastreado y perseguido.

Y hay métodos mucho más sofisticados. Por ejemplo, en los últimos años ha prosperado un tipo de *malware* denominado *ransomware*, que, al infectarte, toma el control de tu ordenador e impide el acceso a tus archivos hasta que pagues un determinado rescate. Algunas versiones de *ransomware* se hacen pasar por una autoridad oficial, como es el caso del temido Reveton Trojan. Este virus bloquea el ordenador infectado, en el que hace emerger una ventana con el emblema del FBI y un mensaje en el que comunica que el propietario de esa computadora ha incurrido en una violación

de las leyes federales contra la descarga ilegal de material audiovisual, o bien que ha reproducido o descargado archivos prohibidos con contenidos pornográficos. Para redimir al atemorizado usuario, se le solicita que abone una multa que oscila entre los 200 y los 400 dólares. Te sorprendería mucho ver el porcentaje de gente que acaba pagando sin hacer demasiado ruido. Muchos de ellos por miedo a la vergüenza de que pudiera trascender qué estaban haciendo en esos momentos con su ordenador.

Esta estafa está tan perfeccionada que se adapta a cada contexto nacional. Por ejemplo, si eres estadounidense te aparecerá el citado mensaje del FBI, pero, si eres británico, la pantalla emergente mostrará el logo de Scotland Yard, o el de Europol, si eres de algún otro lugar de Europa. Incluso tienen versiones en árabe para los habitantes de Emiratos Árabes Unidos y otros países de su entorno. Las víctimas de este *ransomware* se cuentan por decenas de miles en todo el mundo.

Otro troyano que se ha labrado gran fama internacional por su peligrosidad es el conocido como CryptoLocker, que encripta los archivos del ordenador infectado de modo que su propietario no puede leerlos ni acceder a ellos. A continuación, el troyano muestra un reloj con una cuenta atrás y un mensaje siniestro: el usuario tiene sólo 48 horas para pagar 300 dólares o todos sus archivos serán destruidos de forma irreversible. Cerca de 250.000 personas han sido víctimas de CryptoLocker, cuyo creador se ha embolsado aproximadamente 30 millones de dólares. ¿Quién dijo que los informáticos no podían ganar cantidades desorbitadas de dinero?

También en España hemos sufrido este *ransomware*. A principios de 2015, CryptoLocker bloqueó 400.000 archivos del recinto ferial de Madrid, IFEMA, haciéndose pasar por un mensaje de la empresa pública Correos. Y, por las mismas fechas, Deloitte fue víctima de un ataque —paradojas del destino— en el centro de seguridad que tiene en Alcobendas, donde trabajan doscientas personas los 365 días del año.

El ataque fue dirigido a una financiera que enviaba remesas de divisas a otros países a través de una treintena de oficinas en España. Una mañana, todas las sucursales recibieron un paquete

postal personalizado acompañado de un programa informático y una carta firmada supuestamente por el director de la compañía. Todo parecía real. En la carta, el ejecutivo les pedía amablemente que ejecutasen el dispositivo para actualizar los sistemas. Sólo una sucursal lo hizo, pero desató un virulento ataque masivo que inmediatamente provocó el desvío del dinero de cuentas de sus clientes a un banco de Rumanía. Esa jornada perdieron la bonita cifra de 300.000 euros. Y es que tan sólo es necesario un tonto dentro de una organización para que un ataque sea efectivo. Aunque el personal esté bien formado y siga todos los protocolos, basta que una persona abra la puerta para que el «bicho» ya esté dentro. En este sentido, pese a toda la tecnología, en el fondo no hemos avanzado tanto, y seguimos tropezando con las mismas piedras.

En realidad, el caso descrito no es más que una evolución del clásico «timo nigeriano», que consistía en ilusionar a la víctima con una fortuna inexistente y persuadirla para pagar una suma de dinero por adelantado como condición para acceder al botín completo. Antes se calculaba que por cada mil cartas enviadas picaban unas cinco personas. Pero enviar cartas internacionales desde Nigeria tenía un costo significativo. Hoy en día, usando medios tecnológicos, el costo es residual; además, se puede llegar a millones de personas y siempre se encuentra a alguien que abre amablemente la puerta. Luego, si el fraude está bien pensado y bien ejecutado, la efectividad aumenta.

El *malware* que solicita rescates, y cualquier tipo de *ransomware*, también puede integrarse en el sistema operativo de los teléfonos móviles, haciendo que sus posibilidades de infección se multipliquen. Además, sus víctimas no tienen por qué ser sólo usuarios individuales: también pueden ser empresas, asociaciones sin ánimo de lucro o, incluso, agencias gubernamentales.

Esto último fue lo que ocurrió en Massachusetts hace algunos años. Un día, el Departamento de Policía de Swansea fue infectado con uno de estos troyanos después de que un empleado abriera un email malicioso. El departamento fue entonces obligado a abrir una cuenta en bitcoin y pagar 750 dólares para evitar que todos los archivos policiales se perdieran para siempre. Para que te hagas una

idea de que los cibercriminales siempre van un paso por delante, el jefe de la policía de Swansea declaró entonces a la prensa que no tenía ni idea de qué era un bitcoin, ni de cómo diablos funcionaba el *malware* hasta ese momento. Desde luego, tras este ataque no lo volverá a olvidar. Pues así es, querido amigo: éste es el tipo de personas que debe protegernos del crimen del siglo XXI, y también de esos nuevos cibercrímenes y ciberataques que, en muchas ocasiones, ni entienden ni conocen, y contra los que, por supuesto, no tienen siquiera la capacidad de defenderse ellos mismos.

## Cuando el progreso se nos va de las manos

Y es que hemos de reconocer que la tecnología evoluciona a velocidad de vértigo, hasta el punto de pillar con el paso cambiado incluso a las autoridades, como en el ejemplo anterior. El desarrollo técnico sirve, por regla general, para mejorar la vida de las personas, pero también puede tener consecuencias no previstas e indeseadas.

Es lo que ha ocurrido en los últimos años con la tecnología biométrica, o aplicada al reconocimiento corporal. En 2013, Apple lanzó su flamante iPhone 5 con un lector de huella digital. El sistema te permitía usar esta función para desbloquear el teléfono e, incluso, para realizar compras online. No tardó en seguirle los pasos Samsung, cuyo modelo Galaxy S5 también incorporaba el lector de huella digital y permitía, entre otras funciones, validar tu cuenta de PayPal. Por supuesto, ambos sistemas, el de Apple y el de Samsung, no tardaron en ser hackeados. De hecho, hay decenas de vídeos en internet que explican cómo hackear un escáner de huella digital. No es demasiado difícil.

Los cibercriminales más cualificados son capaces de romper la seguridad de los sistemas por medios digitales. Los menos avezados tampoco tienen demasiados problemas para sortear los nuevos métodos de reconocimiento, como ocurrió con una banda de gánsteres de Malasia. Estos, en concreto, consiguieron burlar el escáner de huella digital de los vehículos Mercedes clase S. ¿Que cómo lo hicieron? Muy fácil: cortando los dedos de los propietarios de los coches de lujo con machetes. Sí, es cierto, es un método poco tecnificado y nada sutil, pero intuyo que bastante efectivo.

Aunque no hace falta llegar a ese extremo. Por ejemplo, algunos hackers han conseguido burlar los escáneres de reconocimiento con moldes creados con plastilina infantil. Otros son capaces de recoger las huellas dejadas en una copa de vino y elaborar un molde de gel a partir de ellas.

Algo parecido a esto fue lo que sucedió en Alemania en 2008. El entonces ministro del Interior, Wolfgang Schäuble, había comenzado a promocionar los nuevos sistemas de reconocimiento de huella

digital. En vista de su entusiasmo, los hackers del Chaos Computer Club decidieron darle una lección de ciberseguridad. Tomaron sus huellas de un vaso de agua que había empleado durante una intervención pública y las reprodujeron en un molde de plástico. Concretamente, las reprodujeron 4.000 veces, y repartieron una copia con la revista del club, acompañándola de un artículo en el que se animaba a suplantar la personalidad del ministro.

El sistema no era tan seguro como pensaba Schäuble. No era cierto que nadie pudiera robar tus huellas digitales, como aseguraban los defensores del invento. Y tampoco era verdad que las huellas digitales fueran inmutables, como también sostenían. Esto último lo ayudó a desmentir una joven china de veintisiete años de edad en 2009. Lin Ring había sido repatriada desde Japón, pero estaba como loca por volver allí, así que decidió pagar a un cirujano cerca de 15.000 dólares para que intercambiara sus huellas digitales de la mano derecha con las de la izquierda. Sólo así podría burlar el escáner de entrada en el aeropuerto de Japón.

Y el truco funcionó. Lástima que la policía la descubriera cuando, dos semanas después, intentaba casarse con un hombre japonés de cincuenta y cinco años de edad. Aquello olía a matrimonio de conveniencia, y las cicatrices circulares en torno a las puntas de los dedos de Ring tampoco ayudaron mucho. La joven fue detenida y la policía nipona declaró que era la novena persona arrestada ese año por fraudes relacionados con cirugías biométricas.

Y, si los sistemas de reconocimiento de huellas digitales no son del todo seguros, tampoco podemos decir que lo sea el otro invento biométrico de moda: el escáner de reconocimiento facial. Hace algunos años, en Australia, la policía se enfrentó a un caso insólito. Durante una ceremonia de graduación de nuevos policías, los agentes identificaron a un hombre entre la multitud que llevaba una cámara profesional y un teleobjetivo. Al parecer era miembro de una banda criminal de motoristas, y estaba tomando imágenes de los agentes para crear una base fotográfica de reconocimiento facial para identificar a los policías y poder reconocerlos si participaban en alguna operación encubierta. Los malos son malos, pero no tontos, y

en ningún caso van a renunciar a las ventajas que les abre la tecnología.

Este tipo de prácticas puede tener consecuencias trágicas, y no sólo para policías: imagínate el peligro que tendría en un programa de protección de testigos, por ejemplo.

## Entonces, ¿Bin Laden era un emprendedor?

El desarrollo tecnológico y la globalización han dibujado un escenario laboral muy competitivo, en el que Silicon Valley representa la innovación y la pujanza técnicas. Jóvenes de todo el mundo sueñan con poder sacar adelante su idea, encontrar financiación para su empresa y levantar un gran emporio como Google o Facebook. Vivimos la edad de oro de los emprendedores, y todo el mundo quiere ser el próximo Steve Jobs.

Pero, junto al garaje donde nació Apple, hay otros garajes, algunos de los cuales no están ahí para alumbrar la próxima *startup* de éxito mundial, sino que hacen las veces de laboratorio para el desarrollo de *malware* como el que hemos visto en páginas anteriores y del que se servirá el crimen organizado. Y resulta verdaderamente lacerante que haya bandas de delincuentes llenándose los bolsillos mientras algunos jóvenes luchan cada día por formarse, tratar de contribuir a la innovación tecnológica y mejorar los servicios al alcance de los ciudadanos.

Es el caso, por ejemplo, de San Jain, indio de nacimiento, y su amigo sueco Björn Sundin, dos brillantes emprendedores que, hace unos años, desarrollaron un proyecto tecnológico de gran éxito. En 2006, cuando comenzaba a crecer la preocupación por las ciberamenazas en un escenario ya completamente dominado por internet, estos jóvenes tuvieron la idea de centrarse en el desarrollo de nuevos y mejores antivirus.

Construyeron una empresa con esfuerzo y poco dinero a la que bautizaron Innovative Marketing, y trataron de seguir los pasos de los gigantes digitales. Como HP, Google o Apple, eligieron un país con políticas fiscales amables, en este caso Belice, para registrar su compañía. También trasladaron sus oficinas a Kiev (Ucrania), donde los costes laborales eran mucho menores que en Estados Unidos. Gracias a ello pudieron contratar a grandes ingenieros, informáticos y matemáticos por unos sueldos mucho más bajos que los que habrían tenido que pagar en Silicon Valley.

También invirtieron en publicidad para que la empresa apareciera lo más arriba posible en los motores de búsqueda, y apostaron por

los últimos modelos de afiliación desarrollados por Amazon para atraer nuevos clientes. En definitiva, Jain y Sundin habían construido una empresa seria, que ofrecía un *software* absolutamente novedoso de antivirus y seguridad para ordenadores. Su trabajo fue recompensado, y algunos de sus productos estrella, como Malware Destructor, System Defender o Windows AntiSpyware, contaron sus ventas por millones. Sí, posiblemente ninguno de los dos era el nuevo Steve Jobs, pero lograron un caso de éxito de *startup* de manual, de esos que son celebrados en internet por millones de jóvenes que quieren emular al cofundador de Apple.

Fue tal el éxito de Innovative Marketing, que la empresa recibía más pedidos de los que podía atender, y sus jóvenes fundadores, desbordados, tuvieron que hacer un esfuerzo inmenso para adaptarse a la demanda de sus clientes. Mejoraron su estructura corporativa y contrataron personal para los departamentos de desarrollo de *software*, garantía de calidad, finanzas, cuentas, marketing, recursos humanos, traslado y localización de *software*, investigación y desarrollo, producción, soporte técnico, subcontratación, etc. Y fueron de nuevo recompensados con un éxito absoluto. La compañía se convirtió en una multinacional que operaba en todo el mundo, con más de seiscientos empleados y clientes en más de sesenta países. Contaban con un centro de atención telefónica que atendía las llamadas en inglés en la India, los pedidos en alemán eran encargados a un equipo bilingüe localizado en Polonia, mientras que los encargos en francés se deslocalizaron a Argelia.

Las compras de *software* se podían realizar online, con sólo hacer un clic, y la empresa tenía una política de devoluciones generosa, que llevó a que más del 95 por ciento de sus clientes declarara sentirse «contento» con el servicio de Innovative Marketing. Estaban comprometidos con el buen trato a los usuarios y estimulaban a sus trabajadores ofreciendo premios por objetivos y designando a los mejores empleados del mes. También organizaban actividades extralaborales para cohesionar al equipo, de tal modo que puede decirse que Innovative Marketing no sólo era una empresa muy eficiente, también era un buen lugar para trabajar.

La compañía ingresó alrededor de ¡500 millones de dólares por ventas en tres años!; para ponerlo en perspectiva basta decir que esa cifra era mayor que los ingresos de empresas icónicas como Twitter. Vamos, que la compañía iba como un tiro. Pero te preguntarás qué tiene que ver esta historia de emprendimiento y éxito profesional con el cibercrimen. Y, sobre todo, te preguntarás por qué hablo de Innovative Marketing en pasado: es imposible que una empresa con tal volumen de ventas haya quebrado, ¿verdad? Bueno, agárrate, que vienen curvas.

Digamos que he omitido un pequeño detalle sobre el modelo de negocio del gran proyecto de los amigos Jain y Sundin. Era, más o menos, como sigue. Imagina que un día estás navegando con tu ordenador, revisando tu correo electrónico o cotilleando a tu ex en Facebook, vamos, lo que haces cada día. Todo es como siempre hasta que, en un momento indeterminado, emerge en el centro de tu pantalla un aviso inquietante: *WARNING*: UN VIRUS SERIO HA SIDO DETECTADO. Por si eso no te ha preocupado lo suficiente, por tus altavoces comienza a sonar una sirena de alarma que termina de acojonarte, la pantalla se pone roja y parpadea. Vamos, pasa todo lo que puede pasar, sin llegar a oír tiros ni explosiones cerca de casa.

A continuación, aparece el logo de System Defender, uno de los productos de Innovative Marketing, que, aparentemente, comienza a escanear el ordenador en busca de virus. Su veredicto es descorazonador: «Tu ordenador se encuentra en riesgo inminente de destrucción del sistema y pérdida permanente de toda la información». Tienes veintiocho virus desconocidos, seis gusanos y ocho programas espía instalados. Pero, tranquilo, System Defender te ofrece la solución: «Haz clic aquí para eliminar inmediatamente todas las amenazas».

Habría que ser tonto para no hacerle caso. Así que haces clic, y entonces eres dirigido a una página de Innovative Marketing donde te ofrecen adquirir el System Defender por el módico precio de 49 dólares, con la garantía de que solucionará todos tus críticos problemas. Pero imagina que has sido lo suficientemente tonto como para ignorar la alarma y has decidido que pasas de hacer clic en «eliminar todas las amenazas». Te da igual. Tratas de pinchar fuera

de la ventana emergente, pero el ordenador está bloqueado. El mensaje con la señal de aviso permanece imperturbable en el centro de tu pantalla, y la horrible sirena continúa atronando. El botón de escape no funciona, así que decides reiniciar el ordenador. Buen intento: al arrancar de nuevo vuelves a toparte con la maldita alarma y el dichoso aviso de riesgo inminente. La única salida posible para recuperar el control de tu ordenador es pagar los 49 dólares que cuesta el System Defender de Innovative Marketing.

Este tipo de táctica se conoce con el nombre de *crimeware*, una categoría de productos que designa aquel *software* que ha sido diseñado para cometer delitos. El aviso de alarma era un señuelo, y tu ordenador nunca tuvo ninguno de esos virus que aseguraba el falso escáner. Todo fue fruto de la imaginación del *software* criminal, cuya misión, después de engañarte, era eliminar tu antivirus original, instalarte *malware* y programas espía y, por último, robarte los datos de la tarjeta de crédito empleada para comprar el System Defender a fin de venderlos después en el mercado negro. Además, Innovative Marketing había infectado páginas web legítimas para que cuando algún despistado hiciera clic en ellas fuera infectado con el *malware* que después haría emerger la temida ventana de riesgo inminente y su sirena de alarma.

El pastel se destapó después de que un gran número de clientes se quejara a las autoridades en decenas de países distintos, propiciando una investigación que reveló este gran negocio del crimen organizado en internet. Descubierto el delito, supondrás que Jain y Sundin recibirían un castigo ejemplar, un castigo a la altura del delito masivo que habían cometido. No corras tanto. Nuestros jóvenes emprendedores podrían estar leyendo esto desde algún lugar paradisiaco, mecidos por la brisa, en una hamaca tendida entre dos cocoteros. Efectivamente, nunca fueron detenidos. Sobre ellos pesa una orden de detención internacional, pero lograron escabullirse antes de que el FBI y la Interpol dieran con ellos. Hoy están en la lista de los hackers más buscados por el FBI, y permanecen en paradero desconocido, viviendo de los cientos de millones ocultos que les granjeó el *crimeware*. Desde luego, si existe el cibercrimen perfecto, se parece mucho a Innovative Marketing.

El caso de esta empresa afincada en Ucrania es especialmente espectacular, pero no es el único ni mucho menos. Europol calcula que hay entre cien y mil capos detrás de bandas similares dedicadas al cibercrimen organizado, la mayoría de ellas procedentes de Rusia y Ucrania. La preocupación por estos ciberataques ha aumentado después de que su número creciera un 48 por ciento en 2014, hasta alcanzar la escalofriante cifra de 42,8 millones. Por este motivo ha sido impulsado el Foro Global sobre Ciberexperiencia, un grupo de expertos de 45 países firmantes de la Declaración de Budapest de 2001, el primer tratado contra el cibercrimen.

Respondiendo a la pregunta de este capítulo, Bin Laden no era un emprendedor. Era un grandísimo hijo de puta, pero un hijo de puta idolatrado en algunos países del mismo modo que aun hoy hay otros ciberdelincuentes idolatrados, especialmente en Asia y la Europa del Este, como si fueran empresarios de gran éxito.

## Hacktivistas

A estas alturas del libro es posible que ya te hayas dado cuenta de que en internet nada es lo que parece. No te preocupes, a medida que vayas avanzando en la lectura, esa actual sensación de inquietud será un mero chascarrillo simpático. Incluso dos jóvenes emprendedores de aspecto inofensivo, que podrían ser tus vecinos o tus compañeros de clase, pueden poner en marcha una banda de crimen organizado de alcance mundial. En la era digital, a la hora de buscar culpables, las cosas no son blancas o negras, sino más bien tirando a grises. La distinción entre los héroes buenísimos y los malvados villanos hace tiempo que quedó para las películas de Hollywood. En el mundo real, los gobiernos, las agencias de espionaje, los empresarios, los activistas, los hackers y los delincuentes comunes comparten el uso de ciberataques para obtener sus fines. Internet es ese quinto campo de batalla donde suceden estas acciones, el «quinto elemento» después de la tierra, el mar, el aire y el espacio.

Y en ese quinto elemento hay malos malísimos, pero también hay actores difíciles de catalogar. Es el caso de los hacktivistas (acrónimo de «hacker» y «activista»), cuya actividad ha sido definida en Wikipedia como «la utilización no violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos. Estas herramientas incluyen desfiguraciones de webs, redirecciones, ataques de denegación de servicio, robo de información, parodias de sitios web, sustituciones virtuales, sabotajes virtuales y desarrollo de *software*».

Es decir, los hacktivistas desempeñan una actividad que, en ocasiones, llega al límite de la legalidad, y en otras es directamente ilegal; tanto que nos permite encuadrarlos dentro del apartado de cibercriminales, aunque, al mismo tiempo, aseguren obrar de acuerdo con un compromiso ético y rechazar la violencia, lo cual les ha granjeado millones de simpatías en todo el mundo. Tanto es así, que muchas personas, sin saber muy bien de lo que hablan, se definen en sus perfiles sociales como hacktivistas por el mero hecho de ser contestatarios y reivindicativos.

Bueno, algunos hackers simplemente se meten en problemas por pasarse de graciosos y no calcular bien las consecuencias de sus fanfarronadas. Es lo que le pasó a Chris Roberts, hacker y fundador de One World Labs, que tuvo la genial ocurrencia de bromear en Twitter con la idea de «jugar» con los comandos del avión en el que viajaba de Denver a Siracusa. Por supuesto, nada más aterrizar ya le esperaba el FBI en el aeropuerto, donde fue detenido y le fueron requisados su ordenador y su iPad.

Aunque la cosa no pasó a mayores, la Government Accountability Office (GAO), una agencia estadounidense independiente que realiza estudios estadísticos y auditorías para el Gobierno, ha advertido que tomar el control y trastocar los planes de vuelo de un avión puede ser tan simple como hackear los sistemas del aparato a través de su wifi.

Pero, al margen de anécdotas como la del hacker bromista Chris Roberts, el hacktivismo predica que el acceso a la información en internet debe considerarse un derecho humano fundamental, y tiene sus raíces en la cDc, o Cult of the Dead Cow (Culto de la Vaca Muerta). La cDc es una organización hacker fundada en un matadero (de ahí su nombre) de Lubbock, Texas (Estados Unidos), en 1984.

Bajo el paraguas de esta organización nació el grupo independiente Hacktivismo, dedicado a la creación de tecnología anticensura, así como a promover su Declaración Universal de los Derechos Humanos en internet. Entre algunas de las campañas de ciberactivismo emprendidas por Hacktivismo destacan su colaboración con el grupo Hong Kong Blondes para poner fin a la censura en internet impuesta por el Gobierno de China. También se sumaron a un llamamiento de guerra digital contra el país asiático, así como contra el Gobierno de Irak.

En 2006, además, lanzaron la campaña «Goolag» (un juego de palabras con «Google» y el término «gulag»), en respuesta a la decisión de la compañía de acatar la censura en internet para operar en China. Primero parodiaron el logo del gigante estadounidense para que se leyera «Goolag: exportando censura, una búsqueda cada vez». Y luego también vendieron camisetas y otros artículos de

*merchandising*, cuyos beneficios destinaron a promover los derechos humanos en China. Además, ese mismo año, estudiantes por la liberación del Tíbet respaldados por cDc realizaron una manifestación contra Google en Dharamsala (India), empleando el logotipo de la firma en distintas formas.

La pregunta que siempre sobrevuela cuando analizamos los grupos de ciberactivistas es: ¿el fin justifica los medios? Ésa es la sombra de duda que siempre ha acompañado al grupo de hacktivistas más conocido del mundo: Anonymous. La fortaleza de Anonymous, a diferencia de otras organizaciones de hackers, es que no se trata de una agrupación definida, sino, más bien, de un gran número de grupos e individuos independientes que se conectan por medio de internet y utilizan herramientas digitales para conseguir un objetivo común. Con sus inconfundibles máscaras de la película *V de Vendetta*, son la metáfora perfecta de internet: descentralizados, pero coordinados. La mayoría de quienes actúan detrás de Anonymous ni siquiera se conoce entre sí, lo cual hace todavía más difícil a las autoridades la persecución de este tipo de delitos digitales.

Bueno, excepto en España, donde se dio un caso delirante que provocó risas a escala internacional: en junio de 2011 nos levantamos con la noticia de una rueda de prensa de la policía española en la que nos informaba de que había detenido a la «cúpula» de Anonymus. Desde luego, eso dejaba entrever hasta qué punto no estaban entendiendo nada. A quien realmente habían pescado era a tres chavales, uno en Barcelona, otro en Alicante y otro en Almería, que llevaban a cabo protestas contra la ley Sinde, que pretendía regular los derechos de propiedad intelectual en la red, atacando varias páginas web.

Y el caso es que Anonymous surgió por diversión, pero, con el tiempo, fue adquiriendo tintes de compromiso político, pasando a ser mundialmente conocido por sus campañas contra la censura en internet y los derechos de autor y a favor de la libertad de expresión. Algunas organizaciones han sido blanco habitual de los ciberataques de Anonymous. Éste es el caso de la Iglesia de la

Cienciología (seguro que Tom Cruise todavía tiene pesadillas con ellos, ¡se lo merece por castigar al mundo con las secuelas de *Mission Impossible*!).

La campaña contra la Iglesia de la Cienciología, llamada Project Chanology, comenzó con la difusión de un vídeo en el que aparecía el propio Cruise hablando en términos muy efusivos de la Cienciología (incluso señalaba que sólo quienes pertenecen a esa fe pueden ayudar a una persona después de sufrir un accidente de tráfico). Los responsables de la autodenominada Iglesia trataron de impedir su difusión, alegando que el vídeo era de uso interno exclusivo. Fue entonces cuando Anonymous acusó a la Cienciología de imponer censura en internet e inició una serie de ataques DDoS, chantajes, bromas telefónicas y otras medidas destinadas a paralizar las operaciones de dicha Iglesia.

Otro que debe dormir mal por las noches pensando en Anonymous es Gene Simmons, el líder de la conocida banda de rock *Kiss*. ¿Que cuál fue el pecado de Simmons? Pues amenazar con demandar a todos aquellos que se descargaran su música de forma ilegal. La respuesta de Anonymous fue tirar abajo la web de la banda y difundir toda su obra musical para que su acceso fuera libre.

También grandes entidades como PayPal, Bank of America, MasterCard o Visa han sido blanco de la cólera de Anonymous por colaborar con las autoridades impidiendo pagos y donaciones a Wikileaks.

Pero quizá el peor parado fuera Aaron Barr, quien, en febrero de 2011, era director de la empresa de seguridad informática HBGary Federal. A principios de ese mes, Barr anunció que su compañía había logrado infiltrarse en Anonymous, y que haría públicas sus averiguaciones en una rueda de prensa multitudinaria en San Francisco. Pero aquella rueda de prensa nunca tendría lugar. La web de la empresa fue inmediatamente hackeada por los ciberactivistas, que colocaron su propio mensaje en la página: «Sus recientes reivindicaciones de haber logrado infiltrarse en Anonymous nos divierten, y también lo hacen sus intentos de utilizar Anonymous como un medio para obtener la atención de la prensa». Y terminaban con una advertencia: «Déjanos enseñarte una lección

que nunca olvidarás: no te metas con Anonymous». El ridículo de una empresa que prometía seguridad en la red y no podía garantizar la suya propia fue sideral.

Pero no se contentaron con eso. Anonymous tomó el control del correo electrónico de la empresa, haciendo públicos más de 68.000 correos electrónicos personales, así como la cuenta de Twitter de Barr, en la que publicó su número de la seguridad social y otros datos personales. ¿Ilegal? Seguro ¿Moralmente aceptable? En otros casos, puede; en éste en concreto, no lo parece.

Sin embargo, en la larga lista de criminales hay, sin duda, tipos mucho más malos que estos hacktivistas. Tipos, incluso, con los que a veces se enfrentan estos ciberactivistas. Sucedió con el cártel mexicano de Los Zetas, que secuestró a un miembro de Anonymous un día de 2011. La respuesta de los hackers fue amenazar a los narcotraficantes con hacer públicos los nombres de políticos y autoridades vinculados a ese cártel. Según *The New York Times*, Anonymous podía tener en su poder información de hasta un centenar de los principales «socios gubernamentales» de Los Zetas en México, Estados Unidos y Centroamérica.

Las amenazas de Anonymous no sólo suponían para los traficantes el riesgo de ser detenidos por las autoridades, sino que constituían un verdadero peligro de poder ser asesinados por miembros de cárteles rivales. Tras meditarlo, Los Zetas decidieron poner en libertad al hacktivista secuestrado, eso sí, no sin antes realizar una advertencia: por cada nombre que Anonymous revelara, la banda asesinaría a diez personas. Finalmente, una vez su colaborador fue liberado, los hackers decidieron poner fin a la llamada Operación Cártel, y la cosa no pasó a mayores.

No cabe duda de que las actividades llevadas a cabo por la mayoría de los grupos de ciberactivismo, incluyendo a Anonymous, transcurren principalmente fuera de la legalidad. También es evidente que, en muchas ocasiones, el proceder ético del que se jactan puede resultar discutible. Sin embargo, los chicos de Anonymous nos parecerán unos angelitos si los comparamos con algunos de los cibercriminales que se esconden y operan en internet. De hecho, en mi opinión, la red no es un mundo de blancos y

negros, sino más bien de tremenda variedad de tonos grises. Algunas de las prácticas empresariales de las grandes multinacionales de internet no distan mucho de las que realizan algunos de estos grupos supuestamente delictivos.

Sea como fuere, ya conoces y usas cada día la cara amable de la red, la que te ofrece todos los días Facebook, Twitter y Youtube. Ahora, prepárate para conocer su lado oscuro.

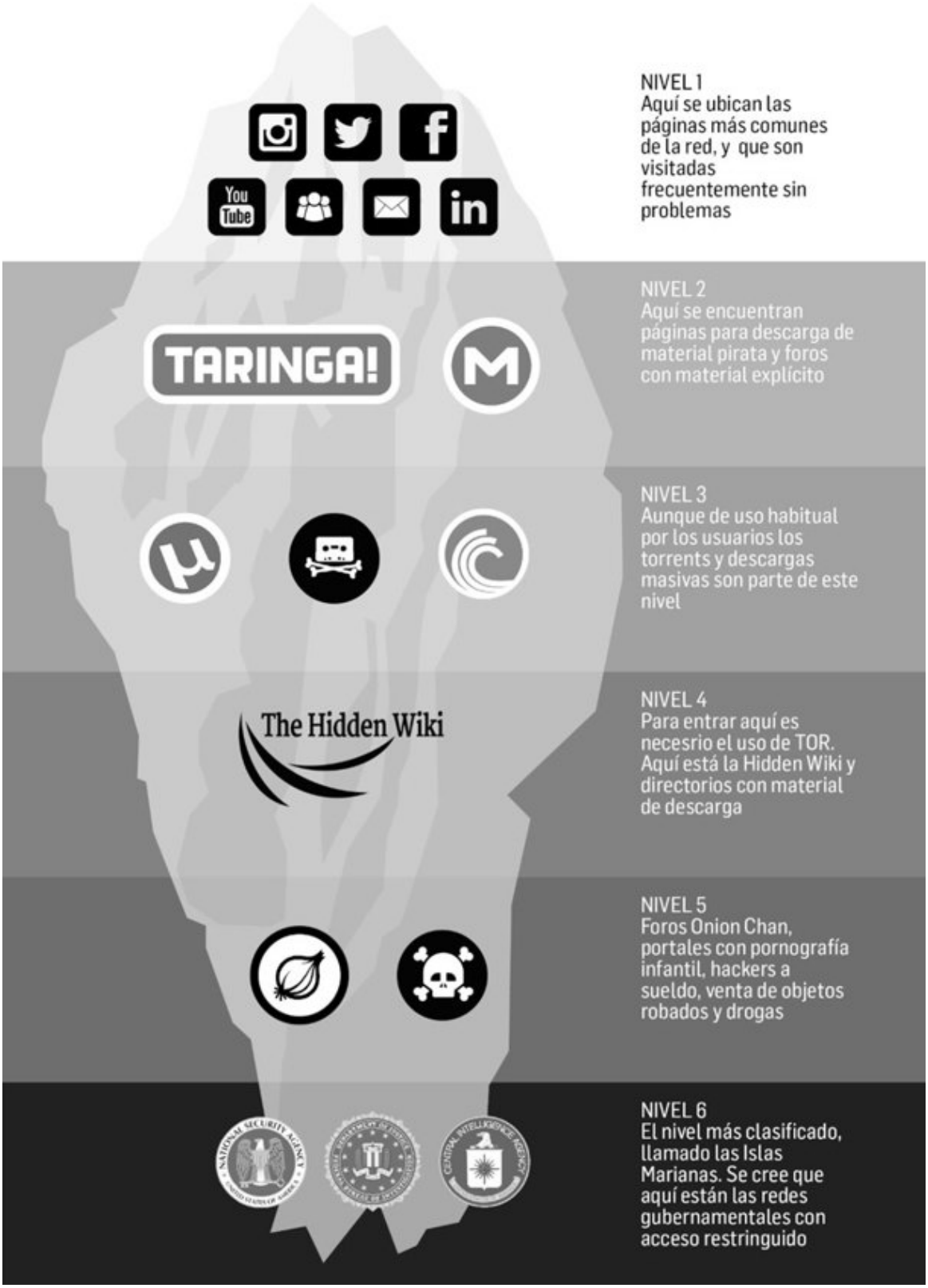
## El lado oscuro de la red: la darknet

Te despiertas y enciendes el ordenador. Subes al metro y tecleas en tu *smartphone*. Crees que el mundo cabe en la pantalla de tu iPad. No hay rincón del universo digital que no pueda barrer tu dispositivo inteligente, no hay información que no puedas encontrar con Google Chrome. Lamento decirte que lo que contemplas desde tu Samsung dista mucho de ser el universo, por mucho que se llame Galaxy.

Todo lo que puedes ver con tu Mac es tan sólo una pequeña superficie emergida en medio del océano: la punta de un inmenso iceberg. Y acabas de colisionar contra él. Bajo la superficie se extiende, como una gigantesca mole de hielo, el 96 por ciento del tráfico de internet, aquel que circula de forma encriptada y no puede ser, por tanto, indexado por los motores de búsqueda como Google o Bing, que sorprendentemente aún existe. Y eso significa que los usuarios no pueden acceder a esa parte de la red. Normalmente.

## Los niveles de la «internet profunda»

Fuente: El Heraldo




NIVEL 1
Aquí se ubican las páginas más comunes de la red, y que son visitadas frecuentemente sin problemas

NIVEL 2
Aquí se encuentran páginas para descarga de material pirata y foros con material explícito

NIVEL 3
Aunque de uso habitual por los usuarios los torrents y descargas masivas son parte de este nivel

NIVEL 4
Para entrar aquí es necesrio el uso de TOR. Aquí está la Hidden Wiki y directorios con material de descarga

NIVEL 5
Foros Onion Chan, portales con pornografía infantil, hackers a sueldo, venta de objetos robados y drogas

NIVEL 6
El nivel más clasificado, llamado las Islas Marianas. Se cree que aquí están las redes gubernamentales con acceso restringuido

El concepto de *darknet*, o «red oscura» (que también se conoce como *deep web*, o «web profunda»), fue acuñado por cuatro ingenieros de Microsoft en 2002. Ese año presentaron un artículo científico en una conferencia de seguridad en Washington al que titularon: «La darknet y el futuro de la distribución de contenidos». Lo que los autores vaticinaban en su trabajo es que la administración de derechos digitales no sería capaz de detener la difusión en internet de contenidos con derecho de autor. La razón residía en el desarrollo técnico: a medida que la tecnología se hace más sofisticada, resulta más fácil compartir contenidos en la red.

En 2002 decir esto no parecía tan obvio como ahora. Hacía menos de un año que se había producido el cierre de Napster, y existía un desconcierto general sobre el futuro de los contenidos compartidos. Napster fue la primera gran red P2P de intercambio (algo así como una «red entre iguales»), la cual ofrecía un servicio de distribución de archivos musicales en formato MP3. Había nacido en 1999, y pronto logró popularidad mundial, llegando a alcanzar cerca de 27 millones de usuarios mensuales.

Lógicamente, Napster no gustaba a las discográficas, que veían cómo, gracias a este servicio, la música sujeta a derechos de autor era compartida libremente, sin coste alguno para el usuario y, sobre todo, sin beneficio para los sellos musicales. Empezó así un periplo judicial de las discográficas contra Napster que llevó al cierre de la red P2P en 2001.

Los usuarios de Napster denunciaron que la posibilidad de compartir archivos era una cualidad propia e inherente a internet, y que el papel de Napster se limitaba a servir como motor de búsqueda de estos archivos, no teniendo responsabilidad en el uso lícito o ilícito que sus clientes hicieran de ellos. Sea como fuere, lo cierto es que Napster cerró, pero sus perseguidores no consiguieron acabar con el problema.

Tras la clausura de Napster, sus usuarios migraron a otros sistemas de intercambio de archivos. Sistemas de *software* como Ares, Kazaa, Emule o eDonkey, que seguramente conocerás, y que es muy posible que tú también hayas utilizado. Los ingenieros de Microsoft que dieron nombre a la darknet habían predicho que, con

el tiempo, las personas se unirían en torno a redes P2P como la difunta Napster, así como por medio de redes locales. Lo que tenían claro es que la difusión de archivos no se detendría con el cierre de Napster, y la aparición de nuevos sistemas para compartir archivos como los que acabamos de señalar venía a darles la razón.

La administración de derechos digitales lo tenía muy complicado para combatir las nuevas tecnologías, pues bastaba un único usuario en el mundo capaz de burlarla para que un archivo musical o una película fueran volcadas a la red y hechas públicas. Había nacido la darknet, y los sistemas P2P constituían el primer nivel sumergido del gran iceberg digital.

Pensarás que, vista así, la darknet no parece tan oscura, y que cualquiera puede descargar un programa para compartir música o películas burlando los derechos de autor. Tienes razón. Pero sigamos buceando, toma aire, que todavía queda mucho iceberg por recorrer.

## Cosas de locos que lo flipas

Hay un estupendo artículo de Matías S. Zavia sobre la darknet que comienza con un diálogo genial de la conocida serie estadounidense de televisión *House of Cards*. Se trata de una conversación entre Lucas Goodwin y un personaje secundario de la serie, y lo reproduzco a continuación por su interés para comprender mejor la red oscura:

—LUCAS GOODWIN: ¿*Deep web*? He oído algo sobre eso…

—PERSONAJE SECUNDARIO: Sí, el 96 por ciento de internet no es accesible a través de los motores de búsqueda habituales. Son inservibles. Se puede encontrar de todo por ahí: porno infantil, blanqueo de bitcoins, drogas por correo, hackers de alquiler...

—LG: ¿Y cómo se accede?

—PS: En realidad es bastante fácil, te puedo enseñar si quieres.

—LG: Sí, tengo curiosidad.

—PS: Lo primero que necesitas es TOR. Algunas personas prefieren I2P, pero creo que TOR es mejor.

—LG: ¿Qué es TOR?

—PS: Te protege mediante servidores proxy, te mantiene anónimo. [...]. Pero te advierto: ojito con dónde haces clic. Ahí hay cosas de locos que lo flipas.

¿TOR? ¿I2P? ¿Bitcoins…? ¡Menuda jerga! Lo mejor será que empecemos por el principio.

Imagina que el tráfico de internet discurriera por el interior de una cebolla gigante, una cebolla con tantas capas que, por muchas que quites, nunca llegas a alcanzar su origen. Eso es más o menos TOR. De hecho, estas siglas corresponden a su nombre, The Onion Router (El Rúter Cebolla).

Como casi cualquier gran avance en el campo tecnológico, TOR nació de la investigación militar. Concretamente, de un proyecto llamado Onion Routing desarrollado por el Laboratorio de Investigación Naval de Estados Unidos. A finales de 2004 pasó a ser

patrocinado por la Electronic Frontier Foundation, la organización de defensa de libertades civiles en el mundo digital, hasta noviembre de 2005. Y, actualmente, el proyecto TOR está en manos de Tor Project una organización sin ánimo de lucro orientada a la investigación y la educación, con base en Massachusetts y que ha sido financiada por distintas organizaciones.

Pero, un momento, para el carro: TOR, la herramienta de entrada a lo más oscuro de la deep web, ¿está financiada por asociaciones filantrópicas? Pues sí. De hecho, TOR ha recibido varios premios para proyectos sociales por permitir a millones de personas el acceso al *software* libre, así como por su compromiso con la libertad de expresión y su contribución a acabar con la censura en el mundo. Por su parte, la Free Software Foundation, además, subrayó la importancia de TOR para permitir movimientos disidentes contra los regímenes dictatoriales de Irán y Egipto.

Suena bonito, ¿verdad? Pero no es oro todo lo que reluce, ni tiene tan buenas intenciones todo el que emplea TOR para acceder a la darknet. Entonces, para que nos aclaremos, ¿qué diablos es TOR? Pues no es una red P2P como las que mencionamos antes, las que permiten compartir archivos digitales. Además, pertenece a un nivel más profundo de la darknet. No se trata de una red entre iguales porque, a un lado, quedan los usuarios de TOR, y al otro, los «encaminadores de tráfico», algunos de los cuales hacen la función de servicio de directorio.

Sí, ya sé que es complicado. Pero, fundamentalmente, lo que debes saber es que TOR (aunque existen otras redes de anonimato, como Freenet o I2P) permite el intercambio de mensajes o archivos entre usuarios sin revelar su identidad, es decir, su dirección IP. Tanto el origen como el destino de la información permanecen encriptados, de tal modo que no es posible (en principio) rastrearlos ni conocer la identidad de quienes participan de esa comunicación.

¿Y quién podría querer encriptar sus comunicaciones? Pues los ciberdelincuentes, desde luego, aunque no sólo ellos. Algunos de los usuarios de TOR son agencias de inteligencia que emplean la red para comunicarse con fuentes que desean permanecer en el anonimato. Otras veces, se trata de empresas que quieren explorar

el sitio web público de su competencia sin que su dirección IP quede registrada. Y en otras ocasiones, TOR es empleado por disidentes políticos en regímenes dictatoriales para evitar que sus gobiernos puedan identificarles y perseguirles.

Antes hemos señalado que la información entra y sale encriptada de TOR, de tal suerte que no es posible, en principio, rastrearla. Y he dicho «en principio» porque, según los documentos de alto secreto filtrados por Edward Snowden en 2013, la NSA habría, supuestamente, conseguido «romper» TOR, descubriendo de este modo las identidades de los usuarios que perseguían el anonimato. Aunque esto no ha sido confirmado, son muchos los que sospechan que la inteligencia norteamericana tiene una puerta trasera de entrada a TOR. Al fin y al cabo, es su juguete, ellos lo desarrollaron, así que no parece descabellado.

Algunos expertos creen que el gobierno de Estados Unidos tolera un cierto umbral de delincuencia en la deep web a cambio de poder tener acceso a los grandes criminales que se exponen en la red oscura. Para que te hagas una idea, según quienes defienden que la NSA controla TOR, en la darknet puede prosperar un pequeño traficante de drogas o encontrar cobijo un pedófilo. Sin embargo, si un individuo anunciara, encriptando sus comunicaciones con TOR, un gran atentado terrorista o un magnicidio inminentes, es probable que tuviera al FBI en la puerta de su casa en pocos minutos.

## Las Páginas Amarillas del cibercrimen

Bueno, ya sabemos qué es la darknet, y que, para sumergirnos en ella, necesitamos descargar TOR o alguna otra red de anonimato. ¿Ahora qué? Ahora ya podemos acceder al siguiente nivel de nuestro iceberg gigante: a la Hidden Wiki (o Wiki Oculta). Se trata de un directorio de otras páginas invisibles, y resulta muy útil para orientar la navegación en la deep web. De hecho, los usuarios de la red oscura la consultan a diario, pues las direcciones cambian con frecuencia de dominio, y TOR sólo es navegable con una lista actualizada de enlaces a mano.

Es cierto que existen más wikis y que hay también algunos buscadores. Sin embargo, la Wiki Oculta se ha convertido en el directorio por antonomasia de la darknet, y gracias a ella podemos hacernos una idea bastante aproximada del tipo de webs y servicios que puede ofrecernos la deep web. Para catalogar estos servicios, tomaremos como referencia la clasificación que hace Zavia.

### *Servicios financieros*

El lado oscuro de internet ofrece una variedad de servicios financieros, desde el lavado de bitcoins, hasta cuentas de PayPal robadas, pasando por tarjetas de crédito clonadas, falsificación de billetes o carteras de dinero anónimas.

### *Monedas virtuales, monedas reales*

Quizá deberíamos empezar por explicar qué es el bitcoin. El bitcoin es una «criptodivisa». ¿Cómo? El bitcoin es dinero P2P de código abierto. ¿Qué? El bitcoin es una red innovadora de pagos. ¿Mande?

Bueno, para que nos entendamos: el bitcoin es una moneda digital. Se trata de una tecnología que permite operar sin una autoridad o banco central, pues la gestión de las transacciones y la emisión de bitcoins es llevada a cabo de forma colectiva por la red.

Fue creada en 2009 por una persona misteriosa (o un grupo de personas) que se ocultaba tras el alias Satoshi Nakamoto. Una persona misteriosa y brillante, pues diseñar la moneda hubo de requerir la resolución de ecuaciones matemáticas endiabladas que precisan de un ordenador muy potente.

Que se trate de una moneda virtual (y, por tanto, intangible) no impide que, como cualquier otra divisa, pueda ser empleada como forma de pago. Como sucede con el dinero convencional que tenemos en nuestro banco, los bitcoins aumentan o disminuyen en nuestra cuenta según hagamos ingresos o gastos. La única diferencia es que no podemos sacarlos de un cajero automático. Además, esta moneda está pensada para que sólo pueda haber en circulación un máximo de 21 millones de bitcoins y su valor ha oscilado entre los 50 centavos de dólar y los 1,240 dólares, pico que alcanzó en noviembre de 2013.

La popularidad del bitcoin ha crecido con los años, hasta el punto de que uno ya puede pagar las copas de la fiesta en bitcoins, reservar un viaje espacial o comprar un coche con esta cibermoneda. De hecho, si fueras griego, creo que podrías confiar a medio plazo más en tu capacidad de compra con bitcoins que con euros. Pero ¿por qué es especialmente popular el bitcoin en la deep web? El bitcoin está fuera del control de cualquier Gobierno, institución o entidad financiera, ya sea de tipo estatal o privado. Si el euro está controlado por el Banco Central Europeo, en Europa, y el dólar es controlado por la Reserva Federal, en Estados Unidos, en el caso del bitcoin el control lo realizan, de forma indirecta mediante sus transacciones, los propios usuarios a través de los intercambios P2P. Además, se trata de un medio de transacción que garantiza el anonimato; ningún documento de identidad es requerido para comprar o vender, lo cual ha hecho de esta criptodivisa el medio de pago preferido para las operaciones fraudulentas, como la compraventa de droga o el blanqueo de capitales.

Efectivamente, el bitcoin es el medio de pago «oficial» de la darknet, aunque no es la única criptodivisa que existe: hay más de setenta tipos de monedas digitales, entre las que destacan el ripple, el litecoin o el dogecoin, y generan un tráfico de transacciones de más de 10.000 millones de dólares al año. Y no sólo existen cibermonedas, sino que también ha florecido un boyante negocio de otras formas de pago similares a PayPal. Firmas como Liberty Reserve, E-gold o Web Money se han convertido en verdaderos PayPal para criminales, ya que facilitan una amplia gama de delitos financieros y lavado de dinero en la red.

Y la nueva generación de criptodivisas ya viene pisando fuerte. Algunos creen que el darkcoin acabará jubilando al bitcoin. Esta moneda puede considerarse como el hermano oscuro y ultrasecreto del bitcoin y ha sido creada específicamente para confundir las compras de los usuarios, combinando cada transacción con las de otros clientes, de modo que resulta imposible atribuir un pago a una persona concreta.

Otra de estas herramientas de pago digital de nueva generación es DarkWallet («monedero oscuro»), que permite realizar transacciones hiperanónimas y que es publicitada por sus creadores sin ningún tapujo como «*software* para blanquear dinero».

## Estafas digitales

El problema que tiene un mercado libre, desregulado y anónimo como el que hace posible TOR en la deep web es que constituye el caldo de cultivo perfecto para el florecimiento de los estafadores; y lo único que te protege como cliente en la darknet es la prudencia. Es cierto que todos estamos acostumbrados al *scam* en internet: estafas más o menos burdas en las que el timador trata de convencernos de que acabamos de recibir una herencia de un príncipe nigeriano o que, sorprendentemente, necesita nuestra vital ayuda para sacar petróleo del golfo de Guinea, por ejemplo; son timos en los que, por supuesto, nunca picamos (o eso espero). Pero en la deep web, el *scam* puede adoptar formas mucho más sofisticadas y sutiles.

Una de estas formas de estafa es la denominada *exit scam*, fraude que ya ha sido bautizado como el «crimen perfecto» de la darknet. Intentaré explicarte cómo funciona. Imagina que eres un vendedor que ofrece sus productos en la deep web. Puedes ser un simple vendedor de café o un traficante de heroína, no importa. Sé que puede parecer exagerado, pero ambas cosas conviven en armonía. Tus clientes te realizan pagos con bitcoins a través de cuentas de correo electrónico encriptadas con TOR, y, a cambio, tú les haces llegar un sobre con la cantidad solicitada de café o, bueno…, de droga. Con el tiempo has adquirido fama de buen vendedor; tus clientes te consideran una persona seria y profesional y confían en ti (sobre todo en el caso del café, ¡joder, espero que no seas un narco!).

Sin embargo, un día decides que quieres dejar el negocio. (Tus razones tendrás.) Puede ser que andes con la mosca detrás de la oreja y creas que la policía te está investigando; puede ser que tu entorno familiar y de amistades haya empezado a sospechar de la procedencia de tus ingresos económicos —no seas imbécil, siempre es raro aparecer de repente con un Lamborghini amarillo—; puede ser que no soportes más la ansiedad provocada por la presión de mantener una actividad ilegal de forma continuada; o puede ser que te hayas enamorado de una chica budista que te ha hecho ver que

lo que haces está muy mal (¡esto no te pasaría si sólo hubieras vendido café!). Por lo que sea, tú has decidido cerrar el negocio y marcharte a casa, o bien a meditar al Tíbet. Hasta aquí todo normal.

Pero hay una tentación grande. La tentación de, antes de desaparecer de la darknet, aprovechar la confianza de tus clientes, largamente trabajada, para estafarles. ¿Cómo? Pues dejando de enviar los pedidos solicitados, pero continuando con el cobro de los pagos durante algún tiempo; digamos, concretamente, hasta que los pobres engañados descubren el timo, lo cual, generalmente, sucede varias semanas después, o tal vez más de un mes.

La existencia de estos estafadores acaba perjudicando a la reputación y la credibilidad de los buenos vendedores, así que la deep web ha desarrollado sus propios medios para evitar el *exit scam* y otro tipo de timos. Una de estas barreras de seguridad es el *escrow*. ¿Qué quiere decir que una tienda anuncie sus servicios con *escrow*? Significa que la tienda se compromete a actuar de intermediaria en el proceso de compraventa, de tal modo que retendrá la transacción de bitcoins hasta que el comprador confirme que ha recibido el producto enviado por el vendedor.

Pero, para entender bien cómo funcionan las ventas de productos en la deep web, será mejor que pasemos al siguiente de los servicios que podemos encontrar en la cara oscura de internet: sus servicios comerciales.

## *Servicios comerciales*

Existe un sinfín de servicios comerciales en la darknet. Uno puede encontrar y comprar casi cualquier cosa allí. Navegando con TOR, descubrimos todo un mercado negro que incluye tráfico sexual, *gadgets* robados, armas y munición, documentación falsa y, sobre todo, drogas. Hay casi de todo: desde cuentas vitalicias de Spotify por dos euros hasta falsificaciones de Rolex o Ray-Ban, pasando por

fusiles de asalto AK-47 (no sé por qué, pero siempre quise tener uno en casa) o carnés de estudiante de universidades privadas.

Pero, como decía, las drogas son el producto estrella de la internet profunda. En los últimos años, y gracias al anonimato que proporcionan TOR y los bitcoin, ha proliferado un extenso mercado de la droga, en el que destacan algunos portales que operan como auténticos Amazon o eBay de los estupefacientes. Quizá el más conocido de ellos sea Silk Road (La ruta de la seda).

Silk Road fue fundada en el año 2011 por Ross Ulbricht, un joven flacucho de veintinueve años de edad y aspecto inofensivo que se hacía llamar Dread Pirate Roberts en la darknet. La figura de Ulbricht está rodeada de polémica y controversia: héroe adalid de las libertades para unos, peligroso delincuente para otros, su corta historia es muy ilustrativa de lo que representa la deep web. Digo corta porque fue detenido en octubre de 2013, después de haber amasado una fortuna de cerca de 500 millones de dólares en los bajos fondos de internet. Y todo en menos de tres años.

Ulbricht era un muchacho de Texas que había estudiado ingeniería y se había especializado en materiales con un máster. Aquella tarde de octubre en que fue detenido, Dread Pirate Roberts estaba en la sección de ciencia ficción de una biblioteca cercana a su casa, en San Francisco, conectado al wifi y tecleando en su ordenador. En un momento de distracción, una mujer se abalanzó sobre el ordenador, mientras media docena de hombres reducía al joven ingeniero, ante la estupefacción general del resto de los clientes y de la dependienta del local, que, confundida, trató de asistir a Ulbricht. Los agentes en seguida aclararon la situación: «Somos el FBI, y estamos realizando un arresto. ¡Sorpresa!».

Pero si los clientes de aquella apacible librería de San Francisco se quedaron boquiabiertos con la detención de Ulbricht, la cara de sus amigos y familiares cuando les comunicaron la noticia fue un poema. Por supuesto, no tenían ni idea. Acusaban a Ross de crear y dirigir una empresa ilegal, y no una cualquiera: «El mercado criminal más extenso y sofisticado de internet hasta el momento». Y nadie sabía nada en su entorno.

Silk Road era mucho más que una web en la que podías comprar drogas, era un emporio de todo lo ilícito. Perfectamente clasificadas por categorías, podías encontrar cualquier tipo de droga en el mercado, acompañada de fotos y descripciones del producto. Y lo mismo sucedía con una gran variedad de productos, como armas, documentos de identidad falsos, pasaportes, licencias de conducir, tarjetas de la seguridad social, herramientas de *hacking* con tutoriales para robar cajeros automáticos y programas de *software* para tomar el control del ordenador de cualquiera. También se anunciaban hackers de alquiler y hasta asesinos a sueldo. Todo.

La madre de Ross no podía creer que su hijo, que siempre había sido un buen muchacho, feliz y sano, fuera ese Dread Pirate Roberts del que hablaban los tribunales y las noticias. Pero, para muchos, Ulbricht se convirtió en un ídolo en cuanto se supo su identidad. Sus seguidores, que le consideraban un «campeón de la libertad», contrario a toda forma de violencia, reunieron un millón de dólares para pagar su fianza, aunque ésta fue denegada por el juez.

Ulbricht era un joven brillante y un prometedor científico, pero un día se hartó del mundo académico y decidió que aquello no era para él. Quería ser emprendedor. En los últimos años se había convertido en un libertario radical, muy próximo a las teorías de Von Mises[2] y la escuela económica austriaca. Quería que su empresa promoviera la libertad, fortaleciera el mercado y debilitara al Estado; y fue así como, en 2010, comenzó a desarrollar la idea de Silk Road.

El mundo de las drogas no le era ajeno, pues en la universidad había experimentado con ellas, especialmente con ácidos y otros visionarios psicodélicos. El problema de Dread Pirate Roberts es que desarrolló una obsesión casi mística con su proyecto. Se sentía como un mesías de la libertad, alguien llamado a cumplir la misión más importante de su tiempo: un elegido. Vamos, que se había vuelto completamente gilipollas, posiblemente porque había abusado más de lo recomendable de los ácidos en la universidad. Y cuando uno se siente iluminado, cree que cualquier cosa está justificada si es por llevar a cabo la misión que le ha sido encomendada. Así, al frente de Silk Road, Ulbricht no sólo hizo posible un mercado libre y anónimo de una infinidad de productos, sino que no dudó en eliminar,

literalmente, a cualquiera que pudiera interponerse entre él y su destino.

La primera vez que Dread Pirate Roberts traspasó todas las líneas rojas fue en enero de 2013. Para entonces, el tráfico generado por Silk Road era tan grande que Ulbricht ya no podía manejarlo solo. Necesitaba ayuda, así que decidió contratar un pequeño equipo de administradores a los que pagaba entre mil y dos mil dólares al mes por atender las operaciones cotidianas del sitio, monitorear la actividad de los usuarios en busca de problemas, atender a los clientes y mediar en las disputas entre compradores y vendedores.

Por supuesto, Ulbricht, como fundador y director del negocio, cobraba bastante más que sus empleados, que enseguida se dieron cuenta de que estaban siendo explotados y que la magnitud del negocio no se correspondía con sus ingresos. Uno de ellos, Curtis Clark Green, que administraba la página desde 2011, estaba especialmente molesto porque consideraba que el salario que percibía era demasiado bajo, y comenzó a robar a Silk Road. Sin duda, Curtis hacía poco honor a su nombre y no debía de ser un gran aficionado al cine. Si hubiera visto los filmes *Scarface* o *El padrino*, o al menos la serie *Los Soprano*, sabría que robar al jefe de los malos no suele ser una buena idea. Cuando Dread Pirate Roberts se dio cuenta de lo que su empleado estaba haciendo, no dudó en contratar un sicario para que lo torturara. Así aprendería modales. Pero después se lo pensó mejor, no podía arriesgarse a que Green acudiera a la policía o difundiera información sobre clientes y proveedores: había que matarlo. Lo que el fundador de Silk Road no sabía es que el sicario que había contratado era en realidad un agente del FBI, que ya le pisaba los talones. Poco después, Curtis Clark Green fue detenido tras recibir un envío de un kilo de cocaína en su casa. Los agentes aprovecharon entonces para fingir la ejecución de Green, enviando a Ulbricht supuestas imágenes del asesinato que, en realidad, era un montaje.

Las fotos de la ejecución que Dread Pirate Roberts creía reales le produjeron cierto disgusto, pero no demasiados remordimientos. Estaba convencido de haber hecho lo correcto, y, tal vez por ello, pronto se aficionó a aquello de los sicarios por encargo. Un día, uno

de los principales distribuidores de droga de la página, que se hacía llamar FriendlyChemist, comenzó a chantajear a Dread Pirate Roberts. Le dijo que tenía una deuda de 500.000 dólares con unos traficantes, y que si Silk Road no la saldaba, haría públicos un montón de datos que había hackeado del sitio web, poniendo en peligro todo el negocio.

Por su parte, Ulbricht se puso en contacto con Redandwhite, el *nick* tras el que se ocultaba el miembro de la banda motera Ángeles del Infierno al que FriendlyChemist debía dinero. Finalmente, Ulbricht y Redandwhite se asociaron a espaldas de FriendlyChemist, y llegaron a un acuerdo para que Redandwhite se encargara de hacer desaparecer a FriendlyChemist. Los asesinos a sueldo localizaron a su víctima en Nueva Columbia, donde vivía con su mujer y sus tres hijos. No les tembló el pulso.

Un problema menos para nuestro autodenominado mesías. Pero la lista de sujetos a eliminar no paraba de crecer. Redandwhite informó a Dread Pirate Roberts de la existencia de un sujeto que se hacía llamar Tony76 y que había colaborado con FriendlyChemist, ayudándole a hackear la información de Silk Road que pretendía filtrar. Ulbricht pagó de nuevo a Redandwhite por su asesinato, así como por el de otros tres traficantes de drogas con los que Tony76 compartía casa y negocio. Así se aseguraría de no dejar ningún cabo suelto, de que no quedara nadie que pudiera ponerle en peligro.

Pero Dread Pirate Roberts cometió más errores de los que pensaba y dejó más pistas al FBI de las que le hubiera gustado. Una vez fue detenido, Silk Road fue clausurada, pero, como si de una hidra degollada se tratara, de su cabeza amputada han ido surgiendo otras nuevas similares, con distintos nombres y directores. El juicio contra Ross, aquel buen chico de Texas que ganó las olimpiadas de matemáticas de su instituto y amaba la libertad, se celebró en febrero de 2015. Fue encontrado culpable de los cargos de narcotráfico, blanqueo de dinero, violación informática y otras cuatro acusaciones criminales que le acarrearon la pena de cadena perpetua.

¿Y qué hay de los seis asesinatos?, te preguntarás. Increíble pero cierto: nada. Los cargos fueron retirados. ¿Cómo es posible? Muy

sencillo. No hay cadáveres. Y tampoco hay nombres. Nadie sabe quién se ocultaba tras los *nicks* con los que las víctimas se escondían en la web profunda, por tanto, no se puede demostrar que nadie haya sido asesinado. Sí se conoce, en cambio, la identidad de la primera víctima, Green, cuyo asesinato fue encargado presuntamente por Ulbricht, pero que sólo fue ejecutado de forma ficticia por el FBI.

El caso de Ross Ulbricht y Silk Road, como decía antes, es muy ilustrativo de lo que representa la darknet: un lugar turbio y oscuro donde, al abrigo de las proclamas bienintencionadas de libertad, asociacionismo y no coerción, florece un mercado de crímenes y cibercrímenes. Y todo eso está a un clic de distancia, para todo aquel que quiera sumergirse en TOR.

La deep web no sólo ha hecho posible que un joven emprendedor de Texas haya puesto en marcha el mayor «eBay» de la droga conocido, sino que pone de manifiesto cuán cerca se mueve este paraíso de la libertad de cibercriminales como los hackers a sueldo, y también de criminales como los asesinos por encargo, cuyas acciones traspasan el mundo digital de unos y ceros y producen daños físicos reales y tangibles.

Alquilar a un hacker o a un sicario es un servicio comercial más de la darknet que podemos encontrar gracias a la Wiki Oculta. Los hackers publicitan su negocio como si se tratara de un coche, un apartamento o un esmoquin: «*Rent a hacker*» («Alquile un hacker»). Así de fácil y simple, un informático europeo utiliza este título para anunciarse. El tipo dice tener veinte años de experiencia en ingeniería social y hackeos ilegales, y, entre sus servicios, ofrece ataques DDoS, *exploits* de día cero, troyanos «altamente personalizados» y *phishing*, todo desde 200 euros.

Otros hackers, como uno que se publicitaba como «Hacker4hire | Cyber crime solution», contaban con una lista de precios desglosada para facilitar la búsqueda de los clientes. Éste, en concreto, ofrecía los siguientes precios:

- Hackear un servidor web (VPS o *hosting*): 120 dólares
- Hackear un ordenador personal: 80 dólares

- Hackear un perfil de Facebook, Twitter, etc.: 50 dólares
- Desarrollar *spyware*: 180 dólares
- Localizar a alguien: 140 dólares
- Investigar a alguien: 120 dólares
- Ciberextorsión: «pedir presupuesto por correo»

Yo diría que debe de haber bastante competencia ya que los precios son muy asequibles.

Y lo mismo sucede con los asesinos por encargo, salvo por el pequeño detalle de que, claro, sus tarifas son un poco más elevadas que las de los hackers. Portales como C'thulhu, Quick Kill o Contract Killer ofrecen el servicio de sus sicarios desde el módico precio de 20.000 dólares. Siempre por adelantado, aunque al final imagino que por política comercial aceptaran un 50 por ciento por adelantado y un 50 por ciento a la consecución, porque quién va a ser tan idiota de mandarles 20.000 dólares así como si nada.

Es posible que algunas de las webs que publicitan estos servicios sean una estafa, y también cabe la posibilidad de que, detrás de no pocas de ellas, esté esperando el FBI con las esposas preparadas a quien trate de contratar un asesino. Sin embargo, no hay duda de que existe un mercado de asesinos a sueldo en la deep web, y prueba de ello es que el propio Ross Ulbricht recurrió a ellos en repetidas ocasiones.

*Anonimato y seguridad*

La historia de Silk Road y Ross Ulbricht demuestra hasta qué punto es crucial el anonimato cuando navegas por la deep web, especialmente para aquellos que están involucrados en actividades delictivas. Para quienes se sienten más preocupados por verificar la seguridad de sus comunicaciones y el secreto de su identidad, la Wiki Oculta ofrece un directorio de páginas en las que es posible encontrar instrucciones para reforzar la privacidad en TOR,

especialmente a la hora de realizar ventas con seguridad o en las transacciones con bitcoins.

Es preciso señalar que TOR sólo encripta el tráfico que sale y entra de la web, no los archivos que se reciben ni los que se envían. Esto significa que la información no viaja encriptada por la red TOR, y, aunque ésta proporciona anonimato, no garantiza una seguridad total. Nada lo garantiza, la seguridad total no existe, es una ilusión. De hecho, ya se han dado casos de gente que crea servidores TOR para «esnifar» (espiar, en la jerga de la deep web) las conexiones. Para solucionar esto, en la deep web existen herramientas que refuerzan la encriptación de archivos. Algunos de ellos son LUKS o TrueCrypt, que se pueden utilizar para cifrar los archivos y así quedar protegido de diversas amenazas.

Además, existe un medio para conseguir ser más anónimo en una red descentralizada como TOR, de modo que rastrear tu dirección IP sea casi imposible (¿hay algo imposible para la NSA?). Esto se consigue encriptando las comunicaciones con PGP (o GPG, en su versión de código abierto), el sistema preferido por los traficantes de droga, por razones obvias.

*Servicios de hosting*

La Wiki Oculta también ofrece un directorio de páginas que proveen alojamiento web y almacenamiento de imágenes, donde se antepone la privacidad. Algunos prohíben subir archivos ilegales y otros no tienen ninguna restricción. Puedes imaginarte que algunos colectivos de criminales, como las redes de prostitución y de pornografía infantil, tienen un gran interés en este tipo de servicios.

*Blogs, foros y tablones de imágenes*

En la deep web, y a través de la Wiki Oculta, podemos acceder a un sinfín de foros de discusión y blogs sobre los temas más variopintos: desde sitios sobre ovnis y extraterrestres, hasta foros de debate sobre viajes en el tiempo o de métodos para copiar en los exámenes, pasando por cosas más desagradables, como las páginas de intercambio de imágenes de pornografía infantil y las webs de temática violenta y *gore*.

Algunas de las fotografías y los vídeos que se encuentran en estos sitios son realmente espeluznantes: asesinatos, mutilaciones, violaciones, torturas y todo lo que tiene que ver con la violencia en general parece resultar muy atractivo para algunos de los navegantes de la darknet. Algunas de estas imágenes se descubre que forman parte de montajes. Otras…, bueno, será mejor que cambiemos de tema.

### *Servicios de correo y mensajería*

Si hay algo que hemos aprendido a lo largo de este libro es que pocas cosas hay más fáciles de espiar que un correo electrónico convencional. Si en la internet más conocida esto ya resulta un problema, no digamos en la deep web, donde muchos de sus usuarios tienen poderosos motivos para querer salvaguardar su identidad, también en sus correos electrónicos.

Por eso, a través del directorio de la Wiki Oculta, podemos encontrar webs que ofrecen algunas soluciones al problema de la privacidad en la mensajería electrónica. Existen direcciones de correo electrónico gratuitas (generalmente sólo ofrecen correo web) y otras de pago, con SSL (Secure Sockets Layer; en español, «capa de conexión segura»), que es un protocolo criptográfico que proporciona comunicaciones seguras.

Pero el producto de mensajería electrónica estrella es sin duda Tor Mail, un servicio de correo que permite tanto el envío como la

recepción de mensajes de una forma completamente privada y anónima. Lo que hace Tor Mail es complicar el camino que sigue la información enviada para que resulte más difícil de rastrear, usando varios servidores para enviar el mensaje y dando un cifrado diferente cada vez que pasa por cada uno de ellos, para acabar llevando el mensaje a un servidor de correo oculto que es el que lo envía al remitente. ¿Complicado? Desde luego.

*Activismo político*

La deep web no sólo sirve de refugio a delincuentes, sino que también representa un paraguas bajo el que actuar con protección para activistas políticos, disidentes y otros grupos de personas perseguidos por delitos de conciencia. En el caso de los regímenes autoritarios, TOR se ha convertido en una herramienta indispensable para que los grupos de opositores puedan organizarse sin temor a ser represaliados por la autoridades de su país.

En los últimos años, la relevancia de lo que mencionamos ha podido observarse en países como Siria, Egipto, Baréin, Libia y otros de los Estados que han protagonizado revueltas sociales en relación con la conocida como Primavera Árabe.

Dentro de este tipo de webs también abunda el intercambio de archivos censurados, el hacktivismo y cosas menos respetables, como una página para organizar «magnicidios financiados en masa» (¿una especie de *crowdfunding* para matar reyes y presidentes?). La anarquía es la ideología predominante en la deep web, como no podía ser de otra forma.

*Secretos de Estado y soplones*

Hay un *mirror* de Wikileaks en la deep web, así como varias páginas donde publicar secretos con poca actividad. La más interesante es una web sobre los túneles secretos de la universidad de Virginia Tech. Me temo que si eres amigo de lo «conspiranoico» no vas a encontrar aquí nada que cambie tu vida en este aspecto.

*Libros*

El directorio de la Wiki Oculta ofrece también enlaces a diversas bibliotecas virtuales de la deep web. Podría parecer que lo último que viene buscando un asiduo del lado oscuro de internet son libros; pero, en la darknet, además de para el vicio, la delincuencia y la depravación, también hay espacio para la lectura, un espacio, concretamente, que hay que medir en varios gigas y en miles de libros electrónicos en distintos formatos. Muchos de ellos están libres de derechos de autor, y otros se distribuyen ilegalmente en descarga directa. Hay ciencia ficción, libros prohibidos, textos políticos, literatura…, pero también manuales de cuestionable propósito ético.

*Páginas eróticas*

Por supuesto, si la mayor parte del tráfico en la internet que todos navegamos es hacia contenidos sexuales, en la deep web no podía ocurrir de otro modo. La Wiki Oculta ofrece links para acceder a páginas eróticas de pago y de libre acceso, con decenas de subcategorías de lo más variado, sin ningún tipo de censura y sin ningún límite moral.

Todas estas cosas, y muchas más que nos dejamos fuera, las podemos encontrar en el gran directorio de la darknet que es la Wiki

Oculta. Llegar hasta aquí ha sido relativamente sencillo: basta con descargar TOR y acceder al listado de direcciones de la Hidden Wiki para poder acceder a cualquier sitio. ¿A cualquiera? Bueno, no exactamente. Todavía podemos sumergirnos un poco más hacia la base del gran iceberg digital que es la deep web. Pero ¿puede haber algo más oscuro en internet que todo lo que hemos comentado hasta ahora? Al parecer, sí. Y digo «al parecer» porque el nivel más profundo de la red oscura está envuelto en penumbra e incertidumbre. Son muy pocos los que tienen el nivel técnico suficiente para alcanzar tales profundidades.

Se dice que la mayoría de quienes osan realizar una inmersión hacia lo más profundo de la darknet suelen acabar en brazos del FBI, pues se cree que es el Gobierno de Estados Unidos quien controla este acceso. A este nivel, el más oscuro de todos, se le conoce como «fosa de las Marianas», por analogía con la fosa homónima del mundo analógico.

Nos chocamos con el gran iceberg y nos hundimos en lo más oscuro de internet, donde uno puede ver cosas que no creería. Llegados a este punto, cabe preguntarse si todavía es posible que la situación se ponga más fea en la era digital. Lamentablemente, sí, es posible. En los próximos capítulos veremos cómo se las gastan los nuevos terroristas, y culminaremos con la visión de una guerra abierta en la que nadie es neutral ni está a salvo. Salgamos de lo más profundo del océano de internet y sequémonos la ropa: el próximo episodio se librará muy lejos de los heladores mares del norte, en un desierto polvoriento y bajo un sol abrasador. Haz las maletas, nos vamos a Irak.

4

# Ciberterrorismo

Estamos en Irak. Es 2007, año que terminará como el más sangriento de la invasión, con más de 900 bajas de soldados estadounidenses, más de 1.800 muertos entre miembros de las fuerzas de seguridad iraquíes y más de 17.000 civiles fallecidos de forma violenta.

Sin embargo, incluso en la guerra hay días relativamente tranquilos, y hoy es uno de ellos. Los jóvenes marines norteamericanos han aprovechado la calma momentánea para sacarse unas fotos en su base de operaciones junto a los nuevos helicópteros AH 64 Apache que acaban de recibir. Poco después, animados por la tranquilidad del día, han compartido sus fotos con los nuevos equipos en redes sociales.

Han sido cuidadosos. Se han asegurado de que los helicópteros no estuvieran clasificados como secreto, y que en las imágenes no apareciera ninguna información que pudiera ser de utilidad para el enemigo, como referencias visuales que permitan localizar el emplazamiento. O eso creen ellos. En realidad acaban de cometer un terrible error. Los soldados no se han dado cuenta de que las imágenes que han difundido, como el 99 por ciento de las que tomamos con nuestros teléfonos móviles, tienen *geotags*, etiquetas de geolocalización a través de las cuales resulta relativamente sencillo determinar las coordenadas exactas, longitud y latitud, en las que una fotografía ha sido tomada.

Desde luego, la localización ha resultado sencilla para la insurgencia iraquí, que, con muy pocos medios, está a punto de asestar un duro golpe a los norteamericanos. Gracias a las inocentes imágenes realizadas por un pequeño grupo de ingenuos soldados, sus enemigos lanzarán un ataque de mortero sobre el lugar exacto donde fueron hechas las fotos, destruyendo, mientras estaban posados en tierra, cuatro helicópteros de última generación del ejército de Estados Unidos.

Dado que cada uno de estos aparatos tiene un precio de 70 millones de dólares, estos *selfies* de los marines tuvieron un coste para su ejército de 280 millones de dólares, lo que posiblemente convierte esos *selfies* en los más estúpidos y caros de la historia, además de haberse convertido en un gran éxito de las fuerzas iraquíes en aquella guerra.

De esta anécdota bélica pueden extraerse varias enseñanzas. En primer lugar, debería hacernos reflexionar sobre el uso que hacemos de internet en nuestra vida cotidiana. Si un descuido como el de los soldados norteamericanos, que creían haber tomado todas las precauciones posibles, puede ocasionar una gran pérdida en vidas y bienes materiales durante una guerra, imagínate la cantidad de facilidades que podemos estar dando a potenciales delincuentes todos los días en Facebook y Twitter, subiendo fotos sin tomar ninguna precaución y facilitando datos e información personal sin pararnos un segundo a pensar en el uso del que pueden ser objeto.

Y es que las redes sociales deben ser usadas con cabeza, y es algo que no suele ocurrir siquiera en el ámbito militar. También pasan cosas como ésta en España, como en el caso de la base militar Coronel Sánchez Bilbao, en Almagro (Ciudad Real). En diciembre de 2014 sucedió un surrealista incidente al dejarse un piloto las llaves de un helicóptero Tigre HAD/E dentro de la cabina (sí, para matarlo). Al no poder acceder al aparato, considerado uno de los orgullos tecnológicos de nuestro ejército, se llamó a un cerrajero de una población cercana. El paisano, posiblemente habituado a otro tipo de trabajos, no se había visto en una como ésa en la vida. Aprovechó la ocasión para inmortalizarse mientras trabajaba dentro y fuera del helicóptero. Parece ser que lo solucionó

a las mil maravillas, pero los nervios en el ejército aparecieron cuando recibieron la voz de alarma que indicaba que habían sido publicadas en Facebook, accesibles para todo el que quisiera verlas, las fotos con los cuadros de mando del aparato. Estas imágenes son muy sensibles ya que a ojos expertos dan información sobre todo el equipamiento del helicóptero.

Tras muchos sudores por lo que podríamos calificar como un *#epicfail* a la altura del anterior de los marines estadounidenses, los mandos militares pidieron al cerrajero que eliminara las fotografías de internet, a lo que el paisano, asustando por la que se estaba montando, accedió rapidamente, eliminándolas de su perfil en Facebook.

Esto nos demuestra que en la red siempre encontraremos más información de la que esperamos, y que, buscando con calma, siempre aparecen muchas sorpresas.

Tal vez eso es lo que debió pensar un analista de ciberseguridad norteamericano después de la redada que acabó con la muerte de Bin Laden en mayo de 2011. El tipo se preguntó cuánta información sería capaz de encontrar sobre la brigada de élite ultrasecreta que había trabajado en la operación contra el líder de Al Qaeda. Consiguió identificar a uno de los agentes a partir de una foto ubicada en el sitio web de su clase de entrenamiento para unidades SEAL (unidades de mar, aire y tierra). Otro de los miembros de la redada fue identificado gracias a una imagen en la que vestía una camiseta del equipo SEAL y aparecía con un grupo de amigos. Después rastreó a los amigos de la fotografía, y también consiguió desenmascarar a varios agentes secretos del FBI.

El analista de ciberseguridad demostró a los perplejos investigados que había más información sobre ellos en internet de la que ellos pensaban. Algo que debería servirnos de recordatorio a todos nosotros.

En segundo lugar, este episodio de la guerra de Irak es muy útil para comprender cómo internet y el desarrollo tecnológico han transformado para siempre nuestra concepción de la guerra y el terrorismo. Hoy en día, cualquier pequeño grupo armado con muy poca infraestructura puede ocasionar un gran impacto sobre un

enemigo mucho más poderoso, tal es el caso de los helicópteros AH 64 Apache de Estados Unidos en Irak.

El terrorismo convencional ha evolucionado gracias a la técnica, dando origen a lo que llamamos ciberterrorismo. El FBI lo define como la realización de «ataques premeditados y políticamente motivados contra información, sistemas de computadoras, programas de ordenador y datos que tienen como resultado la violencia sobre objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos».

En la llamada curva de adopción de la innovación, que es la que se cumple para que los grandes avances tecnológicos lleguen a nosotros de forma masiva, los grupos terroristas estarían considerados como *early adopters*, es decir, aquellos que adoptan rápido las novedades tecnológicas para beneficiarse de las mismas, siempre dentro del primer 15 por ciento de la población, justo tras los que las generan, los innovadores.

La tecnoutopía que se promulga a los cuatro vientos en determinados sitios, como en Silicon Valley, es bonita, pero irreal. La imagen de un joven acudiendo a su trabajo en monopatín con su teléfono móvil de última generación y ocupando un puesto laboral en unas oficinas más parecidas a un parque temático que a un centro de trabajo es divertida, edificante y muy «marketiniana», una visión muy gráfica del *american way of life*. De hecho, creo que si le añadiéramos un sombrero de vaquero y un cigarrillo en la boca a dicho joven, la cosa sería como un anuncio de Marlboro, y estaríamos de vuelta a los años noventa. Sin embargo, hoy, todo eso constituye una visión parcial e idealizada de la realidad de la tecnología. La realidad es mucho más cruda, y el que se queda en esa imagen no hace sino pararse a contemplar la epidermis, obviando que hay un mundo interior mucho más complejo.

Hoy, los terroristas, los gobiernos, las grandes corporaciones y todo tipo de personas y criminales compiten ferozmente por ser los primeros en aprovechar la tecnología y sacarle el mayor partido posible. Según un estudio de Gartner Group, el gasto mundial en ciberseguridad en 2014 fue de 71.000 millones de dólares. Para

2019 se espera que sea de 155.000 millones de dólares. ¿Debemos entonces estar tranquilos por el desarrollo de la seguridad informática? No, en absoluto. Pese al enorme crecimiento del gasto en ciberprotección, que alcanza ya una cifra monstruosa, nada garantiza la seguridad. Los expertos en seguridad saben que no hay nada completamente invulnerable. De hecho, hay sólo dos tipos de sistemas informáticos: los que ya han sido comprometidos y los que lo serán próximamente.

Cuando miras a tu antivirus funcionando correctamente sientes una sensación de alivio que es muy similar a la que produce el agua bendita. En 2012, un estudio del Instituto Tecnológico de Israel, junto con una empresa norteamericana de seguridad llamada Imperva, testó los principales antivirus del mundo contra 83 nuevos virus informáticos. El resultado fue desalentador. Tan sólo el 5 por ciento de los virus fueron detenidos y detectados. Es decir, el 95 por ciento del *malware* pudo comprometer los equipos y hacer impunemente el trabajo para el que había sido diseñado.

¿Cómo interpretar estos resultados? Bueno, podríamos decir que si tu ordenador fuera tu sistema inmunológico y no pudiera detectar ni responder al 95 por ciento de las amenazas exteriores hay muy altas posibilidades de que estuvieras muerto antes de acabar la lectura de este magnífico libro. Y eso sería una pena, ya no tanto por tu salud, ¡sino porque me gustaría que acabaras de leerlo!

El problema viene sobre todo porque la mayoría de los antivirus trabajan con analogías. Detectan código malicioso si ya lo han visto antes (o si han visto algo similar), pero, generalmente, no son capaces de detectar las nuevas amenazas. Esto supone un grado de tecnificación similar al que tendríamos si un guardia de seguridad de una sucursal bancaria sólo sospechara y fuera capaz de detener a un ladrón si le ha visto atracar un banco otras veces. En manos de estas empresas, que han mejorado mucho, es cierto, en los últimos años, está el usuario final. Pero éste, sin inmutarse, mira el icono de su ordenador que le dice «usted está protegido», y sonríe. ¡Cuánto mal hace la publicidad!

En otras palabras, un usuario medio está protegido contra amenazas antiguas, que generalmente llevan meses o años

circulando por la red. Es una obviedad destacar que los grupos terroristas tienen acceso a herramientas más sofisticadas que ésas.

## Una amenaza muy real

La potencial destrucción que ocasionaría un ataque a infraestructuras críticas ha puesto a los gobiernos y los medios de comunicación en alerta. Las fuerzas de defensa de los Estados han visto aumentadas exponencialmente las partidas presupuestarias destinadas a la ciberseguridad, y el número de agentes destinados a labores de vigilancia de la web se ha multiplicado.

El Departamento de Defensa de Estados Unidos ha desarrollado una «cibermisión», que contará con 133 equipos en 2018, la cual se encarga de garantizar la seguridad de sus sistemas informáticos, procurar la defensa de los intereses estadounidenses frente a ciberataques y proveer apoyo ciberlogístico a planes de contingencia y acción militar.

También se han implementado políticas enfocadas a la ciberseguridad, como la creación de centros especializados. Es el caso del Centro Europeo de Cibercrimen (European Cybercrime Center, EC3) o el Centro para la Integración de la Inteligencia contra Ciberamenazas (Cyber Threat Intelligence Integration Center, CTIIC), de Estados Unidos.

En España, el Ministerio de Defensa ha constituido el Mando Conjunto de Ciberdefensa de la Fuerzas Armadas (MCCD), responsable de planear y ejecutar acciones relativas a la ciberdefensa militar en las redes, los sistemas de información y las telecomunicaciones de las Fuerzas Armadas, así como de contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la defensa nacional.

Mientras crece del gasto militar de los Estados en materia de ciberdefensa, el ciberterrorismo ha dado el salto a los titulares de la prensa, dando lugar a decenas de miles de artículos sobre este tema. Sin embargo, hay quien considera que esta sobreabundancia en el tratamiento informativo del ciberterrorismo es excesiva, y su queja se basa ciertamente en un argumento de peso: a pesar de las miles de páginas escritas sobre esta amenaza, hasta ahora, las víctimas que ha propiciado el ciberterrorismo son cero. Ninguna.

¿Significa esto que no debemos preocuparnos por el ciberterrorismo? Nada de eso, la amenaza existe, es exponencial e inmediata, y sólo es cuestión de tiempo que terroristas tecnificados consigan asestar un golpe mortal. La potencialidad de un «ciber 11-S» o un «ciber Pearl Harbor» es absolutamente real. De hecho, ya en 2001, fueron descubiertos en Afganistán unos ordenadores pertenecientes a Al Qaeda en los que aparecieron modelos de presas y *software* de ingeniería que simulaba un fallo catastrófico en los controles.

Eso genera miedo. Y ese miedo se explota. Desde 2001, cada año se realiza una encuesta en Estados Unidos en la que se pregunta a los norteamericanos a qué tienen más miedo. Los estadounidenses, pese a que histórica y estadísticamente tienen mucho más riesgo de morir en un accidente de tráfico, por la caída de un rayo o por ingerir más cervezas de la cuenta, siempre han respondido que su principal miedo es el terrorismo. Bueno, no siempre. En 2013, el 70 por ciento respondió que tenía más miedo a su propio Gobierno que a un ataque terrorista. La mezcla de ambas cosas hace que un Gobierno occidental pueda dictar a su antojo todo tipo de normas y leyes en contra de las libertades personales con la aprobación de sus ciudadanos, máxime si afectan a personas de otros países.

En referencia al miedo y al control, viene a mi cabeza la estructura de control que proyectó en el siglo XVII el filósofo y economista Jeremy Bentham. Se trataba de diseñar la cárcel perfecta, y el objetivo era tener a los reclusos controlados sin tener la necesidad de verlos todo el tiempo. Se construyó una torre en el centro del patio, con un ángulo suficiente que impedía a los reclusos poder ver si había alguien dentro. Alguien que no sabe si le observan pero sabe que puede estar siendo observado, se siente vigilado y siempre será sumiso. Se trata de usar el miedo para que los ciudadanos cumplan, y los tiempos no han cambiado mucho desde entonces.

Los gobernantes fomentan el miedo para evitar que la sensación de falsa seguridad, la misma que te da tu antivirus, les impida

legislar según sus necesidades. Pero eso no quiere decir que el riesgo no esté llamando a nuestras puertas. Es real y existe.

Puede dar fe de ello la policía de Lodz, en Polonia. En enero de 2008, dicha policía tuvo que lidiar con una serie de accidentes muy extraños que hicieron descarrilar cuatro tranvías en un breve plazo de tiempo, provocando doce heridos de diferente consideración. Había algo muy extraño en todo ello. ¿Qué estaba ocurriendo? Sorprendentemente, un joven de catorce años de edad había penetrado en la red de seguridad ferroviaria y, con un mando de televisión casero, había construido un mando infrarrojo capaz de manejar las intersecciones de las vías a su antojo. Pasó meses estudiando el sistema de ferrocarriles de esta población de 800.000 habitantes y construyendo su aparato. Cuando fue detenido declaró que lo hizo sólo por diversión; era un ejercicio técnico que se le fue de las manos. Si un chaval de catorce años de edad puede modificar a su antojo el sistema ferroviario, ¿qué no podrán hacer los miembros de una célula terrorista con medios materiales, financiación y una motivación para ello?

Más recientemente, en mayo de 2015, y a través de Twitter, una cuenta anunciaba que «hackers del ISIS» llevarían a cabo próximamente una serie de ciberataques que «sorprenderían» y «asustarían» a Estados Unidos. No era la primera vez que unos hackers supuestamente vinculados al ISIS causaban el pánico en las redes sociales. En enero de ese mismo año, la cuenta de Twitter del Mando Militar Central de Estados Unidos fue intervenida y utilizada para difundir mensajes que anunciaban la llegada del «cibercalifato» e infundir el miedo entre la población norteamericana.

El Gobierno y los medios de comunicación estadounidenses se mostraron muy preocupados por estas ciberamenazas, pero algunos expertos creen que la preocupación era exagerada. Como se apuntó en un blog estadounidense, Moon of Alabama, es bastante probable que las amenazas no tuvieran nada que ver con los temidos terroristas yihadistas. El Estado Islámico y sus auténticos seguidores nunca utilizan la sigla en inglés ISIS (Islamic State of Iraq and Syria). Y no lo hacen por una razón muy sencilla: en su imaginario, el Estado Islámico no puede ser confinado a las fronteras de estos

dos países. La vocación geográfica del Estado Islámico es universal, como lo es su religión.

Por este motivo, son muchos los analistas que creen que detrás de esa serie de ciberataques se escondían simples «ciberpunks» o hackers gamberros. También hay quien considera que la propia administración Obama podría ser responsable de estos incidentes o, al menos, podría haberse aprovechado de ellos para exagerar la amenaza islamista e infundir miedo entre los ciudadanos.

Pero ¿por qué querría Obama, nuestro premio Nobel de la Paz favorito, atemorizar a los norteamericanos? Todo puede tener una explicación, la de sacar adelante la Cyber Intelligence Sharing and Protection Act (CISPA), algo así como una Ley de Protección y Uso Compartido de Ciberinteligencia. La nueva norma permitirá extender la capacidad del Gobierno para vigilar las comunicaciones en internet, tanto a través de sus agencias como gracias a la colaboración activa con las empresas nacionales. La medida ha sido justificada por la necesidad de reforzar la seguridad nacional frente a ciberamenazas, pero hay quien cree que ésta es sólo la excusa para poner a los estadounidenses bajo vigilancia.

Aunque suene sorprendente, no es tan infrecuente que el Gobierno de Obama sea acusado de tergiversar las causas de un incidente para rentabilizarlas políticamente. Son numerosas las voces que acusan a la administración de Obama de mentir al acusar a Corea del Norte de estar detrás del ciberataque a Sony, y que aseguran que el ataque fue ocasionado por extrabajadores de la propia multinacional. Sea como fuere, este cruce de acusaciones suele quedar en el aire, pues el desarrollo tecnológico hace que sea más difícil rastrear y atribuir responsabilidades en internet. Eso es así incluso para los más avanzados servicios de inteligencia, que cuentan con un presupuesto y unos recursos casi ilimitados.

## La tecnología, ¿amiga o enemiga?

Nada que ver con lo que sucedía hace sólo unas décadas, y no digamos ya en los albores del terrorismo. Imagina las dificultades técnicas que debían afrontar los terroristas de la primera oleada anarquista en el siglo XIX, que tenían que comunicarse a través del correo ordinario mediante el uso de códigos secretos, teniendo que aguardar en ocasiones hasta meses para obtener una respuesta, y siendo el correo un medio relativamente fácil de interceptar para la policía. Hoy en día, encontramos grupos terroristas como Al Qaeda o el Estado Islámico, que encarnan una gran paradoja histórica: están guiados por ideas medievales, pero tienen a su disposición la tecnología del siglo XXI.

La navegación a través de internet hace posible que las comunicaciones sean mucho más rápidas. Pero no sólo eso. También permite difundir ideas de forma viral, siendo más difícil identificar a los responsables gracias al anonimato que provee la red. Internet ha reducido las distancias en el viejo mundo, convirtiéndolo en una aldea global.

Las recetas para la preparación de explosivos pueden encontrarse fácilmente online, y la difusión digital de enseñanzas sobre fabricación de artefactos y tácticas de guerra se ha convertido en crucial en los últimos años, sobre todo desde que los terroristas cada vez disponen de menos campos de entrenamiento a salvo de los ataques con drones.

Los grupos terroristas de nuestros días utilizan el ciberespacio como un medio de bajo coste y bajo riesgo para reunir información de inteligencia. Si bien es cierto que un grupo terrorista no dispone de la financiación necesaria para desarrollar y lanzar al espacio satélites espía que les permitan alcanzar objetivos con precisión milimétrica, también lo es que no lo necesitan. Pueden utilizar los satélites que desarrollan los gobiernos de los países y utilizarlos para sus fines. ¿Ciencia ficción? Nada de eso, cualquiera puede hacerlo con Google Earth. De hecho, así es como planeó y ejecutó el grupo terrorista paquistaní Lashkar-e-Taiba los atentados de 2008 en

Bombay (India), que costaron la vida a 164 personas. Todo ello, simplemente, organizándose por medio de Google.

## El contraterrorismo también tiene ordenadores

Pero internet es un arma de doble filo, y no todo iban a ser buenas noticias para los terroristas. Tal como afirmó el secretario general de las Naciones Unidas, Ban Ki-moon: «Internet es un excelente ejemplo de cómo los terroristas pueden actuar de manera verdaderamente transnacional. En respuesta a ello, los Estados deben pensar y funcionar de manera igualmente transnacional».

Efectivamente, las ventajas que ofrece el ciberespacio a los terroristas también pueden ser aprovechadas por el contraterrorismo. La red permite a los grupos armados conectarse de un modo más rápido y efectivo que nunca antes en la historia, pero también facilita a los analistas de inteligencia realizar un mapa de las redes virtuales que tejen, lo cual les proporciona pistas sobre los miembros y la estructura de los grupos.

Como hemos visto en capítulos anteriores, la capacidad de agencias gubernamentales como la NSA para monitorear información en internet es prácticamente ilimitada, y esta ventaja también la utilizan para combatir el terrorismo, gracias al barrido y filtrado de la mayor cantidad de tráfico virtual posible. Estas agencias están especialmente interesadas en lo que se ha dado en llamar «metadatos», algo así como datos de los propios datos que podemos encontrar en la red. Para que te hagas una idea de lo que quiere decir esto, piensa en una llamada telefónica, por ejemplo. A los rastreadores de metadatos no les interesaría tanto conocer el contenido de la conversación cuanto la naturaleza de la misma. Esto es, información relativa a la hora de la comunicación, su duración, el lugar desde el que ha sido realizada, los números y la identidad de los interlocutores de la llamada, etcétera.

Algo así sucede con internet, donde los metadatos facilitan información sobre la localización geográfica, la hora, la dirección de correo electrónico y otros detalles que pueden ser cruciales cuando se está investigando la actividad terrorista en el ciberespacio. Con estos datos se pueden identificar los patrones, conocer las tácticas y rastrear las operaciones de los individuos puestos bajo vigilancia, incluso aunque traten de esconder su identidad. Además, en algunos

casos, la red puede servir para prevenir el terrorismo, ya que permite la identificación de aquellos individuos que, por su círculo de influencia, podrían ser candidatos a ser captados por las redes de reclutamiento criminales.

Las amenazas, reales o no, pueden ser detectadas por muchas vías. Una de las más obvias son las redes sociales. Una simple broma en Facebook o Twitter puede ser monitorizada y tomada muy en serio.

Leigh Van Bryan era un chico británico de veintiséis años de edad que estaba emocionado con su primer viaje a Los Ángeles. Antes de partir tuvo la ocurrencia de escribir en Twitter que «tenía unos días libres antes de ir a romper América». La palabra «romper», que en su acepción informal británica indicaba que tendría unos días locos en Los Ángeles, vamos que estaría de fiesta todo el día, quizá sacada de contexto puede no ser muy adecuada ante los ojos que todo lo ven.

Van Bryan no sabía cuando aterrizó con su acompañante en Los Ángeles que le iban a recibir unos señores con muy malas pulgas al pie del avión. Armados hasta las trancas, le metieron en una celda junto a unos amables traficantes de drogas mexicanos durante doce interminables horas. Les interrogaron y registraron sus maletas. Cuando por fin comprendieron que la misión de «romper América» podría no ser tan literal les metieron en un avión de vuelta a Inglaterra sin poder pisar más allá de las celdas del aeropuerto. Lo único roto fueron sus ilusiones y sus vacaciones. Desconozco si además les hicieron el mítico tacto rectal al que se expone cualquiera que haga un chiste de más en las aduanas de Estados Unidos.

Para los investigadores, en algunas ocasiones, el trabajo resulta más arduo que simplemente monitorizar redes sociales. Sucede, por ejemplo, cuando la comunicación tiene lugar a través de mensajes que nunca llegan a ser enviados, sino simplemente guardados en la carpeta de borradores de la cuenta de correo electrónico. Esta información está a disposición de múltiples destinatarios que usan una contraseña compartida para acceder a la cuenta. De este modo,

pueden acceder a ella siempre que quieran y leer los mensajes guardados por otros usuarios en borradores o redactar uno sin que la información salga nunca de la cuenta. Es decir, jamás circulará por la red. Además, pueden tomarse otras medidas para evitar la detección, por ejemplo el uso de una terminal de acceso público a distancia, como un cibercafé, para acceder al borrador. Este método fue por ejemplo utilizado en los atentados terroristas de Madrid de 2004.

Pero las agencias de inteligencia no sólo combaten a los grupos terroristas con las herramientas que hemos observado, sino que despliegan un amplio abanico de estrategias contraterroristas, algunas de ellas muy sutiles. Tal como relatan Singer y Friedman en su libro *Cibersecurity and ciberwar*, en 2008 y 2009 las agencias de inteligencia norteamericanas lanzaron ataques contra las principales webs de propaganda yihadista en el aniversario de los atentados del 11 de septiembre para evitar que difundieran el vídeo de celebración de Bin Laden. Sin embargo, en 2010 decidieron cambiar de táctica. Lo que hicieron fue hackear la cuenta de usuario del administrador de Al Fajr, una red de distribución de noticias de Al Qaeda. Después solicitaron a los miembros del sitio que se registraran en Al Ekhlaas, un foro que había sido cerrado el año anterior y que, misteriosamente, acababa de reaparecer. El nuevo foro, claro, no era más que una tapadera para registrar e identificar a los terroristas y sus simpatizantes. Y así ocurrió.

En otras ocasiones, el contraterrorismo utiliza los ordenadores de los propios terroristas para espiarlos. Es lo que le ocurrió a Yaman Mukhadab y el Global Islamic Media Front (GIMF), una red para producir y distribuir propaganda online, que en 2011 tuvo que avisar a sus miembros de que dejaran de descargar el programa de encriptación del sitio web, «Mujahideen Secrets 2.0», porque había sido intervenido.

También fueron hackeadas las redes de la sucursal del movimiento Al Qaeda en la Península Arábiga (AQPA) cuando lanzó *Inspire*, una revista online editada en inglés y cuyo propósito era promover el reclutamiento para la causa yihadista, así como para promover tácticas terroristas. La inteligencia británica consiguió

romper la seguridad de la web, sustituyendo la sección «Cómo se hace una bomba» por recetas de magdalenas. Espías, desde luego, pero con mucho sentido del humor. Y en otra ocasión, los hackers contraterroristas consiguieron reemplazar las instrucciones sobre fabricación de explosivos de una web de tal modo que quien tratara de ponerlas en práctica se volaría a sí mismo por los aires. Macabro, con menos humor, pero muy práctico.

Además, los agentes antiterroristas cuentan en ocasiones con la ayuda desinteresada de ciudadanos anónimos. En Estados Unidos se hizo muy famoso Jon Messner, un empresario de Maryland que consiguió derribar la web de Al Neda, un sitio web perteneciente a Al Qaeda. Para Messner, combatir el terrorismo es sólo un hobby que no guarda relación con su actividad profesional. De hecho, su trabajo consiste en dirigir un negocio de pornografía en internet. Sí, los héroes del siglo XXI pueden tener ocupaciones de lo más peregrinas.

## Ojo: ¡qué te la cuelan por Detroit!

Hemos visto cómo el contraterrorismo puede aprovechar las ventajas del desarrollo tecnológico para combatir el crimen, y también sabemos que ningún grupo armado ha conseguido hasta el momento perpetrar un ciberatentado con consecuencias fatales. Sin embargo, tal como hemos señalado, la potencialidad de un «ciber 11-S» es real. Lo que no sabemos es cuándo serán capaces los terroristas de convertir esa amenaza potencial en acto. Sólo es cuestión de tiempo. Podemos tener la certeza de que muchos de esos actos se están ensayando, probando y perfeccionando hoy mismo.

Sólo entre 2011 y 2013, las intrusiones en sistemas informáticos de infraestructuras críticas aumentaron un 1.700 por ciento. La preocupación por este tipo de ataques es tal que, en 2011, una empresa de suministro de agua de California contrató a un equipo de hackers para poner a prueba la seguridad de su red de ordenadores. Los responsables de la compañía quedaron bastante preocupados cuando comprobaron que los hackers a sueldo habían logrado romper la seguridad de los sistemas en menos de una semana.

Además, que no se hayan registrado víctimas hasta el momento no significa que los distintos grupos terroristas que existen en el mundo no hayan perpetrado ciberatentados hasta la fecha. De hecho, existe un largo historial de antecedentes que no conviene perder de vista, y que nos recuerdan que la amenaza es muy real.

El primer ataque digital a infraestructuras críticas tuvo lugar en 1985, y no nos debe extrañar que se produjera en Japón, una de las mecas mundiales del desarrollo tecnológico. En aquella ocasión, el grupo terrorista Middle Core Faction, una banda armada de ideología izquierdista radical, que nació tras la fragmentación del Partido Comunista de Japón, en 1957, atacó el sistema que controlaba los trenes de alta velocidad nipones. Para ello, cortaron el suministro eléctrico y los cables de control informatizados del ferrocarril, y después interceptaron y perturbaron las radiocomunicaciones de la policía para anticiparse a la respuesta de los agentes y ralentizarla.

Afortunadamente, nadie resultó herido, pero 6,5 millones de viajeros se vieron afectados por el atentado, y la empresa atacada perdió alrededor de seis millones de dólares de la época.

Ya en la década de los noventa, el grupo guerrillero Tigres para la Liberación del País Tamil desató una serie de ataques a través de internet, conocidos como «*mailbombing*», sobre agencias gubernamentales estadounidenses. Esta práctica consiste en inundar una dirección de correo electrónico con grandes cantidades de correos con el propósito de que los servidores de la web donde está alojado se bloqueen y el servicio del sitio quede interrumpido o suspendido. Eran los años noventa, y los ataques eran inocentes y poco sofisticados, aunque bastante molestos.

Durante la guerra del Golfo, mientras aviones armados con municiones de precisión atacaban la red de telecomunicaciones y energía eléctrica de Bagdad, alguien penetró en los archivos militares estadounidenses y alteró las historias clínicas de los soldados. Entre otras cosas, cambiaron la información relativa al grupo sanguíneo de los combatientes, algo que puede ser fatal a la hora de realizar transfusiones de sangre a los heridos en batalla.

El ciberterrorismo se mezcló con el hacktivismo y la guerra convencional durante el conflicto de Kosovo. A lo largo de la contienda, hacker*s* rusos, yugoslavos y norteamericanos inundaron decenas de páginas web con grafitis a favor y en contra de Milosevic o la OTAN. Además, internet fue utilizada para poner en contacto a las distintas facciones dentro y fuera del territorio, así como a quienes apoyaban a uno y otro bando. De este modo, surgieron nuevos foros de discusión sobre la situación política y bélica; la información sobre la guerra trascendió los canales de información tradicionales y la red se convirtió en un nuevo campo de batalla en el que se discutían los nuevos acontecimientos del conflicto y se distribuía propaganda de guerra.

En septiembre de 2008, la Organización Europea para la Investigación Nuclear, conocida como el CERN, reconoció que un grupo de hackers griego, llamado Greek Security Team (GST), había vulnerado la seguridad de su sistema informático. Afortunadamente, el episodio no pasó de ahí y quedó en una anécdota, pero no hace

falta señalar que las consecuencias de un ataque ciberterrorista sobre el CERN podrían tener consecuencias devastadoras.

¿Y en España hay antecedentes de este tipo? Pues sí. En enero de 2005, un hacker fue detenido en Málaga por atacar a través de internet un ordenador del Departamento de Defensa de Estados Unidos. El ciberataque había comprometido la seguridad de un dique seco de mantenimiento de submarinos nucleares en la base naval de Point Loma, en San Diego (California).

Además, altos responsables del Centro Criptológico Nacional, que depende del Centro Nacional de Inteligencia (CNI), han reconocido en repetidas ocasiones que el número de ataques cibernéticos sufridos por nuestro país se ha multiplicado en los últimos años. Algunos de ellos han tenido como blanco sedes institucionales o diversas organizaciones, mientras que otros han tenido como objetivo infraestructuras críticas, y hasta el propio CNI. Esto es muy importante. Vale la pena recordar que en España hay más de 3.700 infraestructuras críticas y otras 5.000 especialmente sensibles por su relevancia en los ámbitos sanitario, energético, de transporte o de telecomunicaciones, y un atentado de gran envergadura contra alguna de ellas podría tener consecuencias catastróficas. El drama de la dependencia tecnológica para un país industrializado es que hay miles de fronteras que defender, y es imposible hacerlo con todas ellas de forma efectiva.

En España, el Centro de Respuesta a Incidentes de Seguridad TIC (CERT), ubicado en León, analiza unos cuatro millones de incidentes diarios, para ello cuentan con una plantilla de unas noventa personas. Su misión es la protección de las infraestructuras críticas. Entre ellas debemos destacar el suministro eléctrico, clave en cualquier incidente. Sin luz no hay ascensores, no hay semáforos, no hay neveras, no hay teléfonos móviles (ya que no podrán ser recargados), etc. La dependencia energética de nuestra sociedad es evidente.

El secretario de Defensa de Estados Unidos, Leon Panetta, declaraba hace pocos meses que «el próximo Pearl Harbor puede ser un ciberataque contra nuestro suministro eléctrico».

Y tiene razón. Éste es un punto tremendamente sensible en las defensas de cualquier país. Y los malos lo saben. ¡Vaya que si lo saben! De hecho, en Estados Unidos, el House of Energy and Commerce Committee realizó un completo estudio en el que una docena de compañías eléctricas reconocían recibir ataques informáticos constantes diariamente. Como dice un experto en seguridad amigo mío, no hay ataques fallidos, sino test de sistema, que sirven para aprender a realizarlos.

En España, desde el punto de vista del terrorismo doméstico, el contraterrorismo ha utilizado internet para llevar a cabo investigaciones contra miembros de ETA, y, más recientemente, se han producido varias redadas contra acusados de hacer apología del terrorismo a través de redes sociales.

Pero sin duda, la mayor amenaza terrorista de nuestros días, esa que tiene un alcance global, es la que representa el islamismo más radical. Occidente ha reforzado sus sistemas de alerta y seguridad para prevenir atentados, pero resulta imposible anticiparse a todas las actuaciones a través de internet.

En Francia lo saben muy bien. El país galo es uno de los más amenazados por el yihadismo, tanto por su implicación en campañas militares en diversos países de Oriente Medio, como por el elevado número de inmigrantes y ciudadanos de ascendencia musulmana que residen en el país.

En abril de 2015, un grupo de hackers que se identificaron como miembros del Estado Islámico realizó un ataque contra la cadena de televisión francesa TV5, logrando tomar el control de la emisión de once canales, sus cuentas oficiales en redes sociales y sus portales web.

Los asaltantes transmitieron mensajes contra la participación de Francia en la coalición internacional frente al Estado Islámico, difundieron propaganda yihadista a través de las cuentas oficiales de las redes sociales pirateadas y filtraron información del personal del portaaviones *Charles de Gaulle*, que participa en la misión de Irak.

Para que te hagas una idea de la envergadura del ataque, TV5 Monde llega a 257 millones de hogares en 200 países. Christophe

Birkeland, director general de Blue CoatNorway AS, y uno de los expertos mundiales en ciberseguridad, señaló entonces lo siguiente:

> El ataque del ISIS a la cadena francesa TV5 ha sido un ataque complejo y realizado por múltiples medios. Es interesante observar cómo el ataque no parece haber utilizado en particular ni técnicas ni *malware* avanzado. El ataque se ha llevado a cabo afectando a una variedad de elementos, como los canales de televisión, la página web y los canales sociales. Esto muestra un alto nivel de acceso y una profunda infiltración en la red de la cadena de televisión. Esto nos indica que ha sido una acción muy bien planificada y que ha requerido de un conocimiento profundo de la red, lo que ha debido de requerir una considerable cantidad de tiempo y de conocimiento para poder ser llevado a cabo. Hay informes que muestran que las credenciales de los administradores de social media fueron comprometidos y que se utilizaron como vía de acceso dentro de la red, pero una potencial amenaza interior no puede ser excluida.

El ciberataque contra TV5 tiene una especial trascendencia si tenemos en cuenta que se trató del primer ataque de estas características reconocido y reivindicado por una organización terrorista.

Pero el peligro que entraña internet ante la amenaza terrorista no reside únicamente en su potencial utilización como vehículo para perpetrar atentados contra personas o infraestructuras críticas. Según el director del FBI Robert Mueller, hay equipos con capacidad de realizar ciberataques en al menos 108 naciones del mundo. Algo muy poco tranquilizador, ya que en el mundo hay 195 Estados reconocidos por la ONU .

Algunos de estos golpes, desconocidos para el gran público, tienen un gran impacto económico. Así ocurrió en 2012 con un grupo terrorista desconocido hasta entonces y autoproclamado como la Espada Cortante de la Justicia. Lograron desarrollar el mayor sabotaje de la historia con un resultado económico demoledor. El objetivo fue el gigante saudí de la industria petrolera Aramco. El ataque tuvo lugar en los momentos previos a una de las fiestas clave del calendario musulmán, el Lailat el Qadr (Noche del decreto), momento en el que Mahoma reveló el Corán a sus seguidores. Al ser fecha festiva, una parte importante de los casi 20.000 empleados de la empresa estaban en casa celebrando junto a familiares y amigos.

Alguien no autorizado aprovechó para acceder e introducir un USB infectado con un *malware* llamado Shamoon en sus sistemas. El virus se replicó rápidamente en los más de 30.000 ordenadores de la compañía, eliminando por completo toda la información a su paso, deteniendo la producción de petróleo en la mayor petrolera del mundo y eliminando todo tipo de información en los ordenadores infectados. Las pérdidas fueron extraordinarias.

## Reclutando imbéciles

Uno de los usos más importantes que las organizaciones armadas dan a la red tiene como objetivo la captación de adeptos a la causa, así como de fondos para su financiación. Que los terroristas del Estado Islámico defiendan la implantación política de ideas religiosas trasnochadas y superadas desde la Edad Media no quiere decir que no estén a la última en el conocimiento y manejo de las nuevas tecnologías, ni que no estén al corriente de las técnicas de comunicación y propaganda más efectivas.

Así, es fácil encontrar en internet *selfies* compartidos por yihadistas armados con fusiles kalashnikov. En las fotos que distribuyen en las páginas de ideología islamista radical y en las redes sociales, los combatientes del ISIS aparecen sonrientes, posando en las lujosas mansiones confiscadas tras la batalla. En sus publicaciones digitales tratan de potenciar, deliberadamente, una imagen idealizada de la yihad, que representan como una forma de vida envidiable, una vía para el empoderamiento personal, arropada por la camaradería y el compañerismo, y en la que la ideología queda relegada a un segundo plano.

Los combatientes del ISIS se muestran como un modelo a seguir para la juventud. Son muchos los adolescentes que sueñan con poder vestir un uniforme militar y poder empuñar armas, y también son muchas las chicas musulmanas que consideran el sumun de la popularidad poder decir que su novio es un soldado del Estado Islámico. Sí, aunque no lo parezca, unirse a la yihad puede resultar *cool* y sexi a los ojos de jóvenes que han sido convenientemente adoctrinados a través de los canales digitales, y, especialmente, de aquellos con menos recursos o que provienen de hogares desestructurados. Esta propaganda que desde nuestro punto de vista y educación occidentales parece burda y ridícula, no sólo funciona, sino que, además, consigue que el ISIS reclute miles de personas en todo el mundo.

En Europa, el número de tarados mentales que se une cada semana al ISIS comienza a ser alarmante. A principios de 2015, se calculaba que eran más de 20.000 los combatientes terroristas

extranjeros que habían viajado para unirse a las formaciones yihadistas. La mayoría de ellos procede de países en los que la población es mayoritariamente musulmana, especialmente del Norte de África y Oriente Medio; pero, para esa misma fecha, ya eran al menos 5.000 los europeos que se habían unido a las filas del Estado Islámico para combatir en Siria o Irak.

Muchos de estos nuevos soldados de la yihad son jóvenes que, aunque han nacido en países europeos, son hijos o nietos de inmigrantes procedentes de países árabes. A menudo, su vida en el país de acogida que eligió su familia no es fácil: han de afrontar problemas como la pobreza, la exclusión social o el desarraigo. Los lazos de pertenencia, fundamentales para cualquier persona, pero especialmente relevantes en la etapa de transición a la edad adulta, son débiles en muchos de estos casos, y es frecuente que se manifiesten conflictos identitarios: un gran número de estos jóvenes no cree pertenecer al país de origen de sus padres, pero tampoco se sienten plenamente integrados en la comunidad europea en la que han nacido.

Estos muchachos pueden ser un blanco relativamente fácil para las redes de captación de los grupos terroristas en internet. Los reclutadores se acercan a su público objetivo utilizando los códigos de su generación, muy conectada con las redes sociales, y empleando su lengua materna.

Así lo decía el francés Abu Abdala G., un apuesto yihadista que pasó por Reino Unido y España. En Siria, rodeado de niños, afirmaba querer «ayudar a los pobres». Un gesto humanitario que nada tiene que ver con las fotografías de cuerpos decapitados que publicaba en su cuenta de Facebook. Su perfil contaba con unos 4.000 «amigos» cuando murió, en julio de 2014. Creo que ya no podrá interactuar con ellos.

Muchas veces, como decíamos, la radicalización es una consecuencia del fracaso social y la exclusión. Sin embargo, en otras ocasiones, la radicalización tiene lugar cuando un joven sensible que se hace preguntas sobre las injusticias encuentra una ideología y un discurso que se presenta como salvador de la humanidad. Así lo señaló la antropóloga Dounia Bouzar, fundadora y directora del

Centro de Prevención contra las derivas sectarias ligadas al islam (CPDSI), creado en Francia en 2014.

Lo que resulta evidente es que, más allá de las motivaciones que llevan a la radicalización de los individuos, en muchas ocasiones el canal utilizado para captar nuevos adeptos a la causa yihadista es internet.

En 1979 se produjo el estallido de la llamada Revolución islámica en Irán, y ésa es la fecha en la que los expertos dan por inaugurada la cuarta ola de terrorismo de la historia, de índole religiosa. La primera oleada terrorista dio comienzo en la década de 1880, fue de carácter anarquista y se extendió a lo largo de un periodo de cuarenta años. A esta primera ola le sucedió una segunda de motivación anticolonial, que se desarrolló entre 1920 y 1960, aproximadamente. La tercera oleada terrorista fue de ideología izquierdista, y afectó, entre otros países, a España, donde sufrimos largamente el terrorismo de ETA.

Como puedes apreciar, una característica común a todas las oleadas terroristas de la historia es que tienen un periodo de activación aproximado de unos cuarenta años. Si tenemos en cuenta los precedentes, cabría concluir que nos encontramos en la última década de vida del terrorismo religioso inaugurado con la Revolución islámica iraní. Pero debemos ser cautos, porque el desarrollo tecnológico ha transformado para siempre no sólo nuestra forma de vida, sino también el modo de hacer terrorismo, sus tiempos, su limitación geográfica y sus posibilidades reales.

Tradicionalmente, la radicalización y el adoctrinamiento en el salafismo tenía lugar en las propias comunidades de los individuos captados. Con frecuencia, esta radicalización se producía en la mezquita del barrio o en la escuela, y partía de personas del círculo social más cercano. Con la universalización de internet, el público objetivo al que se dirigen los reclutadores de las organizaciones terroristas se ha vuelto global, y las estrategias de captación han evolucionado.

En Francia, la autorradicalización a través de internet está a la orden del día, y no sólo entre individuos con antecedentes delictivos. De hecho, dos tercios de las personas que se han autorradicalizado a

través de la red en este país no estaban fichadas por los servicios de inteligencia. Las autoridades alertan de que «los casos prosperan como champiñones», y que estos «afectan cada vez más a las mujeres».

En los últimos años, siete residentes franceses se han inmolado en ataques suicidas en Irak o Siria; a estos países han partido ya más de mil quinientos yihadistas franceses, y se teme que la cifra pueda llegar a unos diez mil a finales de 2015.

Además, las estrategias comunicativas de los reclutadores se han adaptado a los nuevos tiempos: la instrucción religiosa ya no es necesaria. Lo demuestran mensajes del tipo: «Me importa un bledo el islam, voy a hacer mi propia yihad». Los radicales prefieren vender el Estado Islámico como un grupo para triunfar socialmente y en el que el poder, la fama y el dinero corre a raudales.

Además, para que el enrolamiento resulte más atractivo para los jóvenes, elaboran vídeos que imitan la estética de los videojuegos. Uno de estos vídeos mostraba imágenes aéreas, grabadas con un dron, de la ciudad de Kobane, disputada por los kurdos y el Estado Islámico. Según expertos militares, la secuencia imita los gráficos del popular videojuego *Call of Duty*. Estos vídeos alcanzan gran difusión en las redes sociales, que se han convertido en un instrumento de proselitismo que no sólo distribuye propaganda, sino que también permite dar consejos prácticos para que los jóvenes captados puedan viajar para unirse a la yihad sin suscitar sospechas entre sus familiares y las autoridades.

Este enrolamiento virtual es muy discreto, lo cual complica el trabajo de los servicios de inteligencia. De hecho, en la mayoría de las ocasiones, el primer contacto físico de la mayor parte de los europeos con un yihadista no se produce hasta después de haber cruzado la frontera turca con Siria.

## Chateando con el enemigo

Uno de los testimonios más valiosos sobre el modo en que se produce el reclutamiento de jóvenes occidentales por el ISIS es el que ha aportado Anna Erelle, nombre falso de una periodista francesa amenazada de muerte por investigar y publicar los métodos de captación de los terroristas en internet.

Para llevar a cabo su trabajo, Erelle abrió una cuenta de Facebook y Twitter con un perfil falso en el que se hacía pasar por Mélodie, una joven francesa de veinte años de edad y recién convertida al islam, y en cuyo avatar mostraba una imagen de la princesa Jasmine de la película *Aladín*, de Disney. Mélodie era huérfana de padre, y vivía supuestamente en el sur de Francia junto a su madre enferma. Erelle utilizaba este personaje ficticio para entrar en contacto con jóvenes en situación vulnerable frente al adoctrinamiento islamista, así como para introducirse en los círculos virtuales de occidentales radicalizados.

Buceando por la red, Erelle dio con un vídeo en el que se veía a un individuo atractivo de unos treinta y cinco años de edad y vestido con ropa militar. Tras quitarse las gafas de sol marca Ray-Ban, dejaba ver unos ojos oscuros y maquillados con *kohl*.[3] El hombre explicaba en perfecto francés que su nombre era Abu Bilel y que se encontraba combatiendo en Siria. Finalmente, llamaba a todos los espectadores a la *hijrah*, es decir, a abandonar la tierra de infieles para trasladarse a un país musulmán.

Como había hecho en tantas otras ocasiones, Erelle compartió el vídeo en el perfil de Mélodie. Cuál sería su sorpresa cuando, horas después, encontró en su bandeja de entrada tres mensajes del mismo Abu Bilel, que la invitaba a viajar a Siria. La ficticia Mélodie respondió con un nudo en el estómago: había entrevistado a muyahidines otras veces, pero ninguno mayor de veinte años de edad. Bilel parecía ostentar un cargo de cierta responsabilidad en el Estado Islámico, y constituía una gran oportunidad para la investigación de Erelle. La periodista contestó utilizando un lenguaje adolescente y cometiendo intencionadas faltas de ortografía. Se mostró impresionada y dijo que no se esperaba que un yihadí

quisiera ponerse en contacto con ella. «¿No tienes nada mejor que hacer? LOL», preguntó ella divertida.

Bilel le respondió que por supuesto que tenía muchas cosas que hacer, pero que eran las once de la noche en Siria, y que los combates habían terminado hasta el día siguiente. A continuación, y sin dar muchos rodeos, le pidió a Mélodie que charlaran por Skype. Erelle se puso nerviosa. ¿Chatear por Skype? ¿Ahora? No estaba preparada para eso. Uno no tiene la oportunidad de citarse virtualmente con un sanguinario asesino cada día. Así que buscó una excusa y consiguió aplazar la videollamada para otro momento.

Al día siguiente, Erelle llegó a la revista en la que solía colaborar como *free lance* y comentó con el editor lo sucedido la noche anterior. Juntos acordaron continuar la investigación, pero con mucha cautela: aquel reportaje podía poner en peligro la vida de la periodista, y lo primero era su seguridad. Decidieron celebrar un encuentro por Skype entre Mélodie y Bilel, que sería grabado por un cámara llamado André. Para la videollamada, Erelle debía enfundarse un velo islámico y aparentar diez años menos de los que tenía. Trabajó junto con André en la caracterización, ambientaron el salón de la casa de la periodista para que pareciera el hogar de Mélodie, quitaron las fotos familiares de la vista y apartaron cualquier objeto que pudiera permitir la identificación del lugar. André situó estratégicamente la cámara en un ángulo ciego para la webcam del ordenador de Erelle. Finalmente, tras conseguir colocarse correctamente el velo de forma que sólo dejara a la vista el óvalo facial, Mélodie estaba lista para chatear con Bilel.

Encendió el ordenador y comprobó que Bilel ya la estaba esperando: «¿Estás ahí? ¿Hablamos por Skype?». «Estoy lista», respondió la rejuvenecida Erelle, y la cámara comenzó a grabar.

La periodista estaba nerviosa, pero tenía que interpretar su papel de adolescente y, afortunadamente, lo hizo muy bien. Descubrió que Bilel llevaba quince años financiando el terrorismo islamista, y que su papel actual en el Estado Islámico consistía en reclutar adeptos para la causa en Siria. A Erelle le llamó la atención cómo, a pesar del discurso antioccidental de los yihadistas, los combatientes estaban

obsesionados por las marcas de moda occidentales, como Nike, Gucci o Armani. Son asesinos y terroristas, pero no imbéciles.

Bilel estaba decidido a llevarse a Mélodie con él: «Siria es increíble. Tenemos todo lo que queremos. Tienes que creerme, ¡esto es el paraíso! Un montón de mujeres fantasean con nosotros, somos los guerreros de Alá».

También quiso saber si Mélodie solía llevar el velo. Ella dio la respuesta que había leído tantas veces durante sus investigaciones en internet a otras jóvenes conversas. Afirmó que se vestía con ropa occidental por la mañana y, después de despedirse de su madre y salir de casa, se ponía el velo. Bilel se mostró orgulloso y alabó tanto su alma como su aspecto exterior.

Las conversaciones por Skype se volvieron habituales. Bilel comenzó a mostrarse enamorado de Mélodie y trazó con ella un plan para que se reunieran en Siria y pudieran casarse. La joven se mostró vacilante al principio, pero fue dejándose cautivar (en apariencia, claro), por el seductor muyahidín. Finalmente, Mélodie confirmó que viajaría a Siria en compañía de otra amiga musulmana menor de edad. El plan consistía en viajar hasta Amsterdam, donde una mujer del ISIS esperaría a las muchachas para llevarlas después a Siria.

Erelle decidió continuar con la investigación y viajar a los Países Bajos, donde, tras conocer al enlace del Estado Islámico, pondría fin al reportaje. Pero, al llegar a Amsterdam, no había ninguna mujer esperando a Mélodie y a su ficticia amiga. Tal como le había indicado Bilel, Erelle compró un teléfono de prepago y llamó al terrorista. Éste le confirmó que nadie iría a recogerlas, y que debían coger un vuelo más hasta Turquía solas y, una vez allí, tomar otro vuelo doméstico hasta Urfa, desde donde cruzarían la frontera con Siria.

Viajar a Urfa era demasiado arriesgado, pues el ISIS tenía una base de operaciones allí, así que Erelle decidió que era hora de poner punto final a su investigación y a su relación virtual con Bilel. Le reprochó que había incumplido su promesa de que irían a recogerlas a Amsterdam y se mostró insegura sobre la continuidad del viaje. Ante las quejas de la joven, el terrorista cambió el tono dulce de enamorado de las últimas semanas para mostrar su lado

más autoritario: «¿Te crees que soy idiota? —le espetó—. Soy parte de una organización terrorista, no me puedes hablar así. A partir de ahora te vas a callar. Tú no sabes quién soy yo. Mando sobre cien soldados todos los días. Ni siquiera te he contado una cuarta parte de la verdad. Hay una orden de búsqueda internacional contra mí, por eso ni siquiera puedo ir a nuestras ciudades en Turquía. Sólo puedo viajar a Irak. Tengo 38 años, y tú y tu amiga no me vais a joder. Será mejor que tengas cuidado».

Erelle decidió que ya era suficiente. Puso punto final a las comunicaciones con Bilel, que a las veinticuatro horas ya acusaba su falta de noticias: «¿Dónde estás, pequeña zorra? Te juro por Alá que me las pagarás». Erelle regresó a casa, eliminó todas las huellas de su vida virtual, a excepción de la cuenta de Skype, y envió a Bilel un último mensaje para no despertar sospechas, en el que se disculpaba por no haber podido viajar a Siria.

Una semana después, la periodista publicó su reportaje en prensa, dando comienzo un nuevo periplo para ella: la policía la obligó a cambiar varias veces de número de teléfono por su seguridad, también tuvo que cambiar su lugar de residencia, y fuertes medidas de vigilancia fueron implementadas en sus lugares de trabajo. Erelle tuvo que renunciar a volver a escribir sobre el Estado Islámico, e incluso se vio obligada a deshacerse de su mascota, pues se trataba de un perro de una raza muy poco habitual fácilmente reconocible.

La policía solicitó a la periodista que mantuviera abierta su cuenta de Skype para poder llevar a cabo investigaciones antiterroristas. Cada vez que la abría, Erelle encontraba decenas de amenazas de muerte, entre ellas las de una mujer que decía ser la esposa de Bilel. Dejó de abrirla. Poco después supo que pesa una fetua[4] contra ella.

De Bilel poco se sabe. Al angelito se le dio por muerto durante algún tiempo, pero recientemente se ha sabido que continúa vivo. Tiene diversos antecedentes en Francia por robo a mano armada, y en 2003 se unió a la yihad y se marchó a combatir a Irak y Siria, donde conoció y estrechó lazos con el líder del ISIS, Abubaker al Bagdadi. Tiene tres esposas y, al menos, tres hijos menores de trece

años de edad. Los dos mayores ya están combatiendo en el frente sirio.

Esta historia la conocemos porque dio la casualidad de que, un día, el encargado de reclutar jóvenes occidentales para la causa yihadista en Siria tuvo la mala fortuna de intentar captar a una periodista de incógnito. Pero no sabemos cuántas otras veces tuvo éxito en su empresa. Podemos imaginarnos que muchas, porque, como él mismo reveló en varias ocasiones a Mélodie: «Soy realmente bueno en mi trabajo».

Sucesos como éste han despertado mucha preocupación en los países occidentales, especialmente en aquellos que, como Francia, tienen una mayor población de origen árabe susceptible de caer en redes de radicalización. La creación en Francia de la nueva Dirección General de la Seguridad Interior (DGSI) tiene como objetivo, sobre todo, el reclutamiento de ingenieros para mejorar la detección en internet de estos candidatos y de los reclutadores. Además, las grandes redes sociales como Facebook y Twitter, aunque no vigilan, cierran las cuentas que incumplen las condiciones de utilización, especialmente en el caso de incitación a la violencia.

Por otro lado, algunas entidades privadas han comenzado a ofrecer servicios de monitorización de la actividad terrorista en internet. Es el caso de Search for International Terrorist Entities (SITE, Búsqueda de Entidades Terroristas Internacionales), con sede en Estados Unidos, o la red global Internet Haganah (*haganah* significa «defensa» en hebreo). Ambas monitorizan y reúnen información de código abierto relacionada con organizaciones terroristas. En la práctica, SITE funciona como un servicio de inteligencia que se financia en buena medida a través de suscripciones.

Internet Haganah, por su parte, rastrea y monitorea las actividades en internet de grupos extremistas islámicos con el fin de detectar y bloquear el acceso a los contenidos relacionados con el terrorismo. Esta entidad privada se financia en parte mediante donaciones, y funciona fundamentalmente sobre la base de las aportaciones de una red de voluntarios. Su servicio de monitorización permite investigar e identificar tanto los contenidos

de internet que guardan relación con el terrorismo como las páginas web que alojan dicha información. Una vez realiza la detección, los hallazgos pueden ser puestos en conocimiento de las autoridades policiales o del público. También se puede proceder a solicitar la retirada de los contenidos o el bloqueo del acceso al sitio web en cuestión.

Como señala la ONU, SITE e Internet Haganah son dos modelos de uso y funcionamiento de estos servicios de monitorización diferentes, pero ambos permiten «la rápida detección de los contenidos relacionados con el terrorismo en internet, lo cual puede ser útil para la coordinación de la inteligencia, la investigación y el enjuiciamiento de tales actividades».

Como Francia, también Alemania se ha dotado de armas jurídicas que prohíben la comunicación por texto, imágenes o sonido de todo lo relacionado con el ISIS, sobre todo en las redes sociales. Pero los reclutadores han ido todavía más lejos, y el jefe del espionaje alemán, Hans-Georg Maassen, ya ha alertado del creciente uso de aplicaciones de telefonía móvil como Whatsapp o Instagram para reclutar a nuevos combatientes del Estado Islámico.

Las autoridades alemanas estiman en unos 400 el número de alemanes o ciudadanos residentes en Alemania que han sido reclutados por el yihadismo, de los cuales, unos 130 han regresado al país después de haber pasado por campos de entrenamiento del radicalismo islámico. Se teme que estos 130 individuos puedan ser miembros de células terroristas durmientes, o bien futuros lobos solitarios, por lo que se les mantiene en estrecha vigilancia.

Para llevar a cabo el reclutamiento en internet, el ISIS explota lo que ya se conoce como «yihadismo romántico», que consiste en establecer un mayor contacto virtual con individuos considerados como proclives a dejarse tentar, y, a partir de ahí, en ganarse su confianza.

## Financiación del terrorismo en internet

Pero las aplicaciones para móviles y las redes sociales no sirven a los terroristas únicamente para captar adeptos a su causa y difundir propaganda. También se han convertido en una creciente fuente de obtención de financiación.

Las organizaciones terroristas y sus partidarios usan internet para financiar actos de terrorismo mediante cuatro tipos de estrategias diferentes: la recaudación directa, el comercio electrónico, el empleo de los servicios de pago en línea y las contribuciones a organizaciones benéficas.

La recaudación directa se lleva a cabo por medio de sitios web y chats de temática yihadista, así como a través de campañas masivas de correo y comunicaciones dirigidas a simpatizantes para solicitar donaciones.

El comercio electrónico se convierte en una fuente de financiación del terrorismo cuando los sitios web son usados como tiendas online que ofrecen libros, grabaciones de audio o de vídeo y otros artículos a los simpatizantes, y parte del dinero de cuyas ventas se destina a patrocinar atentados.

Por su parte, los servicios de pago online que ofrecen algunos sitios web o plataformas de comunicación especiales permiten la transferencia electrónica de fondos entre las partes. Estos traspasos de fondos suelen hacerse mediante transferencia bancaria electrónica, tarjeta de crédito o sistemas de pago alternativos ofrecidos por servicios como PayPal o Skype. Los servicios de pago online también pueden ser explotados por medios ilegales, tales como el robo de identidad o de tarjetas de crédito, el uso fraudulento de las telecomunicaciones, el fraude bursátil o los delitos contra la propiedad intelectual.

Otra vía de financiación más creativa viene del saqueo de ciudades cuyas antigüedades y obras de arte acaban en manos de coleccionistas privados, cuyo dinero acaba pagando y financiando (con o sin su conocimiento) las operaciones terroristas del ISIS. Algunas ciudades sirias como Apamea, Ebla o Raqqa han sido completamente saqueadas con este fin.

## Aprendiz de 007

Un ejemplo del uso de ganancias ilícitas para financiar actos de terrorismo es la causa del Reino Unido contra Younes Tsouli. Durante casi dos años, Tsouli, o mejor dicho Irhabi007, su seudónimo en la red, fue una auténtica pesadilla para los servicios de seguridad europeos y norteamericanos. Con sólo veintidós años de edad, Tsouli estaba considerado «el padrino» del ciberterrorismo. Irhabi007, que viene a significar en árabe «terrorista 007», en una alusión a James Bond, fue, entre 2003 (cuando apenas tenía veinte años de edad) y 2005, el principal *webmaster* de las páginas de Al Qaeda, especialmente de su rama iraquí.

Tsouli nació y creció en Rabat, donde se educó en el liceo francés. Cuando era adolescente, decía que quería ser médico o arquitecto, aunque sus compañeros aseguran que era demasiado vago para alcanzar cualquiera de los dos objetivos: «Fumaba porros sin parar e introducía alcohol en sus latas de coca-cola», recuerda uno de ellos. Algún profesor más benévolo lo definía en términos cariñosos como «un chaval solitario, sensible y algo rebelde con el que se podía, a veces, dialogar».

Tsouli nunca llegó a terminar el bachillerato en Rabat, porque a su padre lo destinaron a Londres, donde fue nombrado director de la oficina de turismo de Marruecos en el Reino Unido. Allí se matriculó en informática en el Westminster College, y frecuentó la mezquita de Shepherd Bush, donde entró en contacto con las redes de Al Qaeda y se radicalizó.

Poco después comenzó a trabajar para la organización terrorista desde su dormitorio, en el apartamento que compartía con su padre en el oeste de Londres. Tsouli no sólo contribuyó a financiar en internet el que por entonces era el grupo criminal más temido del mundo. Con la ayuda de sus dos compinches compró 180 dominios de internet, abrió páginas web en las que colgaba vídeos —la decapitación del norteamericano Nicholas Berg fue descargada medio millón de veces—, llamó a hacer la yihad, organizó foros encriptados de debate, recaudó dinero de musulmanes piadosos, ofreció manuales sobre la fabricación de explosivos y enseñó a miles

de internautas cómo disimular su identidad. Y hay mucho más, pero, por razones de seguridad, algunas de sus «hazañas» no fueron desveladas durante su juicio.

El FBI y Scotland Yard lo temían más que a cualquier otro combatiente, y *The Economist* llegó a afirmar que «era mucho más importante que cualquier kamikaze». Sin embargo, tal como el propio Tsouli reconoció ante el juez, el acusado sólo manejó «el teclado de su ordenador y no bombas». La cuestión es si, a estas alturas del siglo XXI, alguien duda ya de que un ordenador es un arma. Y puede ser de las más peligrosas. Un equipo con conexión, sobre todo si es manejado por alguien sumamente formado, puede hacer hoy en día exponencialmente más daño que cualquier arma de fuego por masiva que esta sea.

El juez no lo dudó, y por eso lo sentenció en 2007 a diez años de cárcel. La sentencia fue la primera en el Reino Unido por incitación y apología del terrorismo a través de internet, e incluyó a los dos cómplices de Tsouli, el británico Waseem Mughal, al que le cayeron siete años, y el emiratí Tarik al Daur, condenado a seis años. Curiosamente, hasta su detención, los tres sólo se conocían virtualmente. Primero se declararon inocentes y después acabaron por admitir su culpabilidad.

Pero ¿cómo contribuyeron Tsouli y sus dos compinches a financiar el terrorismo internacional? Introduciéndose en bases de datos o mediante una estafa por correo electrónico conocida como *phishing*, Daur consiguió apropiarse en internet de los datos de 37.000 tarjetas de crédito de las que el trío sólo utilizó unas 1.400 —una de ellas de un reservista del ejército de Estados Unidos— para hacer compras por valor de 2,7 millones de euros. Tal como detallaba Ignacio Cembrero en un artículo aparecido en *El País*, «adquirieron desde GPS hasta gafas de visión nocturna —todo ello en venta libre—, un material que podía servir a los yihadistas». Además, Tsouli llevó a cabo campañas para conseguir aportaciones económicas de donantes privados.

Como señala un informe de las Naciones Unidas, los beneficios extraídos del robo de las tarjetas de crédito fueron blanqueados por varios medios, incluida la transferencia mediante el pago online por

E-gold, que se utilizó para dirigir los fondos a través de varios países antes de llegar a su destino. El dinero blanqueado se usaba para financiar tanto el registro por parte de Tsouli de 180 sitios web que hospedaban vídeos de propaganda de Al Qaeda como el suministro de equipo para actividades terroristas en varios países.

Su servicio a Al Qaeda era tan importante que incluso Abu Musab Zarqawi, quien fuera el jefe de la rama iraquí de la organización terrorista, le hizo llegar a través de su secretario un mensaje personal de agradecimiento: «Hermano Irhabi007, has hecho encomiables esfuerzos para difundir nuestro mensaje y servir a la yihad y al Todopoderoso».

Tsouli era todo un maestro en ocultar su identidad, y la policía no hacía más que dar palos de ciego tratando de encontrarlo. Casi nada sabían de él, aparte de que exhibía un comportamiento adolescente: era descarado y cometía frecuentes faltas de ortografía cuando escribía en árabe, aunque no así cuando lo hacía en inglés o francés, idiomas en los que había creado páginas web para inmigrantes musulmanes en Europa.

Cuando por fin lograron atrapar a Irhabi007 no fue por haber cometido un error mientras navegaba por el ciberespacio: fue casi por casualidad. Resulta que en el ordenador de Mirsad Bektasevic, un adolescente bosnio de origen sueco detenido en Sarajevo en octubre de 2005, aparecieron vínculos que conducían a él y a otros cuarenta jóvenes musulmanes. Pocos días más tarde, los agentes de Scotland Yard irrumpieron en el piso donde vivía Tsouli y, tras una breve pelea, lo detuvieron. En aquel momento todavía ignoraban que el muchacho que llevaban esposado a comisaría era nada menos que el célebre Irhabi007 a quien tanto habían buscado. Sólo cuando lograron romper las claves y abrir su ordenador portátil comprendieron que habían dado con el pez gordo del ciberterrorismo.

Además de las formas de financiación flagrantemente delictivas como la que acabamos de describir, en otras ocasiones, la financiación del terrorismo internacional llega por cauces aparentemente legítimos. Es el caso de organizaciones aparentemente benéficas, que tras las siglas ONG desvían con

impunidad fondos hacia fines ilícitos. Se sabe de algunas organizaciones terroristas que han establecido empresas fantasma, disfrazadas de entidades filantrópicas, para solicitar donaciones en línea. Estas organizaciones pueden afirmar que apoyan causas humanitarias, cuando, en realidad, utilizan las donaciones para financiar actos de terrorismo. La ONU advierte de que, entre las organizaciones aparentemente benéficas que se emplean con fines terroristas cabe mencionar la Benevolence International Foundation, la Global Relief Foundation y la Holy Land Foundation for Relief and Development. Todas ellas, asegura, pese a sus nombres inocuos, utilizan medios fraudulentos para financiar organizaciones terroristas en Oriente Medio. Sin duda hay muchas más, y se crean cada día.

Otro modo de obtener financiación cuando los terroristas no son capaces de contar con el apoyo de las organizaciones o no pueden constituir su propia fundación benéfica consiste en infiltrarse en filiales de organizaciones de beneficencia, que utilizan como tapadera para promover la ideología del grupo terrorista o para prestar apoyo logístico y material a sus facciones militantes.

Como puedes ver, en el terrorismo, como en el amor y en la guerra, todo vale. Literalmente. Y lo de la guerra tendrás ocasión de comprobarlo en el próximo capítulo.

5

# Ciberguerra

## La guerra no es un juego, chavalote

En 1983 se estrenó *Juegos de guerra,* un *thriller* dirigido por John Badham. La película, ambientada hacia el final de la guerra fría, cuenta la historia de un joven hacker que se dedica a romper la seguridad de los sistemas informáticos sólo por diversión. Hasta que un día, el juego se le va de las manos al muchacho y penetra involuntariamente en el Departamento de Defensa de Estados Unidos. La broma dará lugar a una crisis que estará a punto de desencadenar nada menos que la tercera guerra mundial.

Esta historia no tiene nada de particular hoy, cuando estamos acostumbrados a las noticias sobre hackers y sabemos cómo se toma Estados Unidos cualquier intrusión, por pequeña que sea, en sus sistemas de ciberdefensa. Pero, cuando se estrenó, hace más de treinta años, *Juegos de guerra* fue clasificada como una película de ciencia ficción. Esto significa que, en un plazo muy corto de tiempo, muchas de las cosas que teníamos catalogadas como fantasías se han hecho realidad. ¿Cuánto tiempo tardarán en hacerse realidad esos ciberataques terroristas que los más escépticos juzgan hoy como un escenario de ciencia ficción? Me atrevería a decir que muy poco.

Lo que estaba anunciando John Badham en *Juegos de guerra* no es sino la conquista del último campo de batalla conocido. Primero fue la tierra; después, el agua; y más tarde sería el aire. A estos tres escenarios bélicos tradicionales se sumó, precisamente en la guerra fría, el espacio. Pero, con el desarrollo tecnológico y la caída del telón de acero, el viejo mundo dividido en dos bloques ideológicos, el occidental capitalista contra el soviético comunista, dio paso a un nuevo orden donde las rivalidades estaban menos definidas y los ataques podían ser mucho más sutiles.

La irrupción de internet como quinto campo de batalla, como quinto elemento, ha hecho la guerra más compleja que nunca. La ciberguerra es un gran conflicto en el que a menudo no sabemos quién es el enemigo que nos ataca, y esta incertidumbre ha conducido a los Estados a tomar una medida concreta de precaución: considerar que todos son enemigos.

A pesar del recelo generalizado, todavía encontramos alianzas virtuales de países, como la que sellaron China y Rusia en mayo de 2015, y que constituye un pacto de no agresión digital. Uno no puede evitar evocar el famoso pacto Ribbentrop-Molotov, aquel acuerdo germano-soviético de no agresión, firmado pocos días antes de que estallara la segunda guerra mundial. El pacto Ribbentrop-Molotov saltaría por los aires en 1941 con la Operación Barbarroja, el nombre en clave para la estrategia de invasión de la Unión Soviética por parte de los ejércitos de Hitler. No me extrañaría que la alianza ruso-china acabara, de modo parecido, en una batalla de Stalingrado digital, máxime teniendo en cuenta que, en internet, los ataques y el espionaje se pueden llevar a cabo de forma anónima, de manera que ambas partes pueden encontrar incentivos para romper el pacto sabiendo que será prácticamente imposible que se descubra.

## Cisnes negros

Como ocurre con el alcance potencial del ciberterrorismo, los escépticos dudan de la capacidad destructiva de una ciberguerra mundial. Sucede, sin embargo, que en todas las épocas ha habido escépticos y que, con no poca frecuencia, han tenido que lamentarse de su falta de previsión. Así pasó, por ejemplo, hace un siglo, cuando, en vísperas de la primera guerra mundial, muchos políticos e intelectuales del momento descartaban que el conflicto pudiera tener lugar. Consideraban que la guerra se había vuelto demasiado costosa para los Estados, que era un lujo que ya nadie se podía permitir. Lo que pasó poco después es de sobra conocido por todos.

También en España hemos pecado de miopes a la hora de anticipar conflictos. Pocas semanas antes de que estallara la guerra civil, ningún político había advertido el peligro inminente, a pesar de que las tramas e intentonas golpistas eran conocidas por el gobierno de Azaña desde hacía varios meses.

Y algo parecido sucedió el 11 de septiembre de 2001 con el atentado terrorista que derribó las Torres Gemelas y costó la vida a cerca de 3.000 personas; a pesar de que ya había el precedente de un atentado contra el World Trade Center, y a pesar de que los servicios de inteligencia tenían información que podía haber puesto en alerta a las autoridades, nadie supo ver lo que se avecinaba.

La primera guerra mundial, como la guerra civil española o el 11-S, fueron «cisnes negros». La teoría del cisne negro fue desarrollada por Nassim Nicholas Taleb para definir aquellos acontecimientos difíciles de predecir que, sin embargo, tienen un impacto dramático en el devenir de la historia. Taleb explicaba que las personas tenemos sesgos psicológicos que nos vuelven individual y colectivamente ciegas a la incertidumbre e inconscientes de la trascendencia que un evento extraño pueda tener.

La ciberguerra mundial puede también entrar en la categoría de cisne negro, habida cuenta del gran número de escépticos que cuestionan su posibilidad. Hay incluso un libro del profesor inglés Thomas Rid titulado *Cyber war will not take place* («La ciberguerra

no tendrá lugar»), de 2013, cuyo título es un préstamo de la famosa pieza teatral de Jean Giraudoux, *La guerra de Troya no tendrá lugar*. Es curioso que Rid haya tomado el título de la obra de Giraudoux para argumentar que una ciberguerra no se producirá, pues todo el mundo sabe lo que pasa al final de la obra del dramaturgo francés: la guerra de Troya tiene lugar. Es más, la guerra de Troya es un acontecimiento bélico histórico.

## Una guerra sin tiros

El razonamiento de Rid y de otros escépticos como él se basa en lo que ellos consideran que debe ser una definición de guerra. La guerra, siguiendo a Clausewitz,[5] debe ser sangrienta; debe ser como el título de aquella película de David Cronenberg que protagonizaba Viggo Mortensen: *Una historia de violencia*. Ellos creen que los ataques cibernéticos no son, por regla general, violentos. Creen que es muy improbable que un ciberataque pudiera tener el impacto que tuvieron Pearl Harbor, el 11-S o Hiroshima en su momento.

Sin embargo, tal como apuntó Walter Laqueur, consejero del Centro de Estudios Internacionales y Estratégicos, en Washington quizá no sea de importancia primordial la cuestión de que «la guerra implica violencia» si los ataques cibernéticos logran infligir daños inaceptables al enemigo aun sin matar a nadie. El fin último de un Estado que libra una guerra no es el de producir la violencia por la violencia, sino el de alcanzar un objetivo político y/o económico. La guerra siempre se ha tratado de eso: intereses; y la violencia es sólo un medio en el camino hacia su consecución.

Además, históricamente, no todas las guerras han implicado violencia física directa. La guerra fría se basó en una carrera de armamentos nucleares que garantizaba la destrucción mutua asegurada de los dos polos rivales; es decir, estaba movida en mayor medida por la disuasión que por la violencia. De hecho, hay quienes creen que es posible trazar algunos paralelismos entre aquel periodo y la actualidad. David Rothkopf, director de la revista de relaciones internacionales *Foreign Policy*, opina que tal vez estemos entrando en una nueva guerra fría tecnológica, tanto por el carácter remoto de los ataques como por el hecho de que pueden ser llevados a cabo indefinidamente sin necesidad de disparar una sola bala.

Efectivamente, el concepto de ciberguerra nos obliga a cambiar el chip respecto a las guerras convencionales a las que estamos acostumbrados. El hecho de que una guerra digital no haya sido declarada no significa que no se esté librando, del mismo modo que la ausencia de un tratado de paz no impide que un conflicto llegue a

su fin. Estados Unidos nunca declaró oficialmente la guerra a Corea del Norte en 1950, pero, por más que el presidente Truman se esforzara en disimularla (llegó a referirse a ella como una mera «acción policial»), es difícil negar que un conflicto en el que murieron 3,5 millones de personas pudiera ser otra cosa que una guerra.

## Tiempos modernos, guerras modernas

En realidad, la última vez que Estados Unidos declaró oficialmente una guerra fue el 5 de junio de 1942, con su entrada en la segunda guerra mundial. Y de eso ya hace casi ochenta años. Tenemos que comprender que el mundo, y la guerra con él, han cambiado mucho desde entonces. El que fuera jefe de contrainteligencia de la NSA, Joel Brenner, dijo en una ocasión: «En Estados Unidos tendemos a pensar en la guerra y la paz como si se tratara de un interruptor con dos posiciones, encendido y apagado; como si sólo pudiera haber una guerra a gran escala o una paz absoluta. La realidad es diferente. Ahora vivimos en un permanente estado de conflicto entre naciones que rara vez desemboca en un enfrentamiento armado. Tenemos que acostumbrarnos a que incluso países como China, con los que indudablemente no estamos en guerra, están en intenso ciberconflicto con nosotros».

Pero, en cualquier caso, resulta altamente cuestionable que la ciberguerra no implique violencia o, al menos, que no vaya a implicarla muy pronto, tal como aseguran muchos de los escépticos.

En 1982, hace la friolera de 33 años, un gasoducto soviético en Siberia explotó como consecuencia de algún tipo de sabotaje cibernético, dando lugar a la mayor explosión no nuclear jamás registrada. Se habla de una potencia de tres kilotones, que lo destruyó completamente. La explosión fue de tal magnitud, que fue el primer fuego visto desde el espacio. No fue Hiroshima, pero no estuvo nada mal, vaya. Se supone que alguna agencia norteamericana estaba detrás de este sabotaje.

El Dossier Farewell, desclasificado en 1996, hablaba de cómo en ocasiones, como parecía ser el caso, la CIA dejaba que la Unión Soviética consiguiera tecnología defectuosa a la que se había incorporado un «caballo de Troya» para controlar su funcionamiento. El exconsejero de Seguridad Nacional estadounidense Thomas C. Reed documenta la operación en su libro *At the abyss: an insider's history of the Cold War* («Al borde del abismo: historia de la guerra fría contada desde dentro»), de 2004; en él explica que «el *software* del oleoducto que manejaba las bombas, turbinas y válvulas estaba

programado para descomponerse. Debía restablecer las velocidades de la bomba y la configuración de la válvula para producir presiones muy superiores a las aceptadas por las juntas de tuberías y soldaduras. El resultado fue la explosión no nuclear más monumental de la historia».

La realidad es que ni atacante ni atacado confirmaron que esto había sucedido, pero hoy podemos considerarlo como el primer acto de guerra cibernética del mundo.

## Guerra 3.0

Dice Laqueur que, «si, como dijo Clausewitz, la guerra es la continuación de la política por otros medios, la ciberguerra es la continuación de la guerra tradicional por otros medios». Así es, la ciberguerra es como una versión mejorada de la guerra convencional, como una guerra 3.0. La ciberguerra aúna elementos de los conflictos clásicos con elementos de sabotaje, *hacking*, espionaje y ataques cibernéticos que facilita internet. Por volver a Clausewitz, la ciberguerra sí que es una «guerra total».

Se estima que cientos de miles de soldados digitales trabajan en misiones de ciberguerra en todo el mundo. De ellos, las tres cuartas partes lo hacen en labores ofensivas y no defensivas. En el ciberespacio sigue imperando la máxima tradicional de la guerra y del fútbol: la mejor defensa es un buen ataque.

Estados Unidos no se posiciona en el bando de los escépticos con respecto a la guerra. De hecho se posiciona en el extremo opuesto: el alarmismo. Los norteamericanos están convencidos de que los ataques cibernéticos a gran escala son muy probables, y saben que el daño que podrían causar es enorme.

Por ello crearon cibercomandos. La tarea de los USCYBERCOM es «planear, coordinar, integrar, sincronizar y conducir actividades para: dirigir operaciones y defender las redes de información específicas del Departamento de Defensa; prepararse para (y dirigir, cuando se indique) operaciones militares que barran todo el espectro del ciberespacio, con el objetivo de permitir acciones en todos los dominios; asegurar la libertad de acción en el ciberespacio de Estados Unidos y sus aliados, y denegársela a todos los enemigos».

Estos cibercomandos cuentan con una fuerza de cerca de 60.000 cibersoldados, y sus cuarteles generales están en Fort Meade (Maryland). ¿Te suena el sitio? Sí, efectivamente, los USCYBERCOM están situados junto a las oficinas centrales de la NSA. ¿Casualidad? De ningún modo. Ambas agencias comparten recursos y personal. Comparten, por ejemplo, a los cientos de doctores en ingeniería, matemáticas, informática y otros campos que trabajan para el Gobierno. Por compartir, comparten hasta el director. El almirante

Michael S. Rogers sustituyó al general Keith Alexander al frente de ambas instituciones en 2014, cuando Alexander se jubiló.

Algunos consideran que este hecho es normal, dada la convergencia de responsabilidades que tienen las dos entidades; pero también hay quien considera preocupante que se difuminen las fronteras entre un comando militar y una agencia de espionaje civil.

En cualquier caso, los USCYBERCOM han experimentado un crecimiento muy rápido dentro del ejército de Estados Unidos, tanto en lo que se refiere a su tamaño como por lo que respecta a su peso específico. Basta señalar que, en 2014, el Gobierno estadounidense dobló el presupuesto destinado a estos cibercomandos, mientras recortaba todas las demás partidas del gasto militar.

Los objetivos de esta ciberfuerza son cinco: «Tratar el ciberespacio como un campo de batalla comparable a la tierra, el espacio, el aire o el mar; implementar nuevos conceptos de seguridad para vencer en este campo; aliarse con otras agencias y con el sector privado; tejer relaciones de colaboración con aliados internacionales; y desarrollar nuevos talentos para espolear la innovación sobre cómo los militares deben luchar para ganar en este campo».

Como parte de esta misión, los USCYBERCOM han creado tres subtipos de ciberfuerzas: las «fuerzas de ciberprotección», para defender las redes de ordenadores del ejército; las «fuerzas de misión de combate», que dan apoyo a las tropas sobre el terreno; y las «fuerzas de misión nacional», que colaboran en la protección de infraestructuras críticas.

En realidad, la labor de estos cibercomandos puede resumirse en las palabras de un antiguo oficial de la NSA: «El objetivo es asegurar que las capacidades de Estados Unidos siguen siendo más avanzadas que las de sus potenciales enemigos», una máxima que también es aplicable a cualquier otra facción del ejército estadounidense. Y añade: «Cualquier cosa que los chinos puedan hacernos, nosotros podemos hacerla mejor».

Es decir, se sigue tratando del viejo concepto de «disuasión» de la guerra fría. Pero hay letra pequeña. La idea es mandar a sus adversarios el mensaje de que el ejército de Estados Unidos tiene la

intención de luchar y ganar en el ciberespacio, pero (siempre hay un pero) «se reserva el derecho de jugar a un juego distinto si no le gusta el resultado». O, como dijo un oficial norteamericano: «Si nos tiras abajo el sistema eléctrico, a lo mejor te metemos un misil por tu chimenea».

El problema de emplear la disuasión en el ciberespacio es que conlleva varios requisitos difíciles de asegurar. Primero, es difícil garantizar la hegemonía en el ciberespacio. Segundo, para poder disuadir a tus enemigos tienes que saber quiénes son, algo que no siempre resulta fácil en internet. Tercero, es posible que la disuasión funcione con los Estados, pero no está tan claro que sea así en el caso de los actores no estatales.

Los actores no estatales no siempre son racionales e, incluso cuando lo son, su balance de costes y beneficios no es el mismo que el de un Estado con fronteras y ciudadanos que defender. Muchas veces, estos actores informales no tienen una localización fija a la que dirigir un ataque y, aunque la tuvieran, no pocos de ellos estarían encantados de ser contraatacados. Una respuesta de Estados Unidos les proporcionaría publicidad y reconocimiento.

## Estados Unidos vs. China

El Congreso de Estados Unidos definió a China como «el actor más amenazante del ciberespacio». Me encantan esos eufemismos porque lo que quieren decir es más amenazante para el poder de Estados Unidos en el ciberespacio. Les encanta hablar del enemigo, cuando se refieren a "su enemigo". Para que te hagas una idea, la rivalidad entre Estados Unidos y China en la era de internet es asimilable a aquella que unía a la URSS y a los norteamericanos durante la guerra fría. Sin embargo, a pesar de la demonización de la que son objeto (con cierta razón) los chinos en este aspecto, lo cierto es que China es el país que sufre el mayor número de ciberataques del mundo. Algo que ver con esto tiene el hecho de que, en ese país, el número de usuarios de internet haya crecido desde menos de un millón, en 1997, hasta unos 700 millones en la actualidad. Sí, en China hay tantos usuarios de internet como en los siguientes cinco países por población conectada, o sea, como en Estados Unidos, Japón, Rusia, Brasil y Alemania juntos.

China suele quejarse amargamente por ser el blanco de la mayoría de ciberataques y, aunque es verdad que los estadounidenses no son precisamente unos angelitos en el ciberespacio, las cosas son un poco más complejas de como las presentan los chinos. El 95 por ciento del *software* que usan los ordenadores chinos es pirata. Esto significa que no cuentan con las últimas actualizaciones de seguridad ni los parches que tienen quienes usan una licencia legal. China tiene razón cuando se presenta como víctima del *hacking*, pero la culpa es en buena parte suya por despreciar la propiedad intelectual, y no ya tanto del espionaje patrocinado por otros Estados.

En cualquier caso, si para Estados Unidos China es «el actor más amenazante del ciberespacio», la consideración que los asiáticos tienen de los norteamericanos no es más amable. Así lo expresó un trabajador del Gobierno chino: «Estados Unidos, que tanto tiempo ha intentado jugar el papel de víctima inocente de los ciberataques, se ha convertido en el mayor villano de nuestra era».

No seré yo el que defienda a los chinos. Presumen de atacar por medio de internet al resto del mundo, y de robar todo tipo de detalles militares, tecnológicos y empresariales. Ahora bien, no es muy diferente de lo que hacen el resto de los países, y cito muy especialmente a Estados Unidos. Al menos, el amigo chino da la cara abiertamente. Los estadounidenses, muchas veces, se ofrecen a colaborar con otros países aliados, que cuando se quieren dar cuenta no encuentran su cartera.

Unos y otros se acusan hipócritamente, pues ninguno de los dos es una hermanita de la caridad precisamente. En el año 2013, Snowden demostró que la NSA había hackeado los sistemas de la prestigiosa Universidad de Tsinghua, en Pekín. El suceso es de especial relevancia, porque esta universidad es una de las seis columnas vertebrales que conducen el tráfico de internet por todo el país. Estados Unidos también pirateó la sede de Pacnet en Hong Kong, una de las mayores compañías de fibra óptica de la región Asia-Pacífico.

Pero China no se queda atrás, y no puede decirse que esté indefensa frente a la amenaza norteamericana; sabe que, en internet, parte de una situación de desventaja por una sencilla razón: se trata de un invento norteamericano. Y los estadounidenses han apelado a la vieja ley no escrita de tantos patios de colegio: mi balón, mis reglas. Así, diez de los trece nodos de servidores que son esenciales para el funcionamiento de toda la red de internet están alojados en Estados Unidos. ¿Y los otros tres? Pues en países que son aliados de Estados Unidos, claro; concretamente en Suecia, Japón y Países Bajos. Pese a ello, debo añadir que cada vez hay más independencia de redes por miedo a Estados Unidos; es por ello que cada vez pasa menos tráfico regional de Latinoamérica o Asia por ese país, por el convencimiento de sus autoridades de que sus redes son absolutamente tóxicas.

Sin embargo, la otra cara de la moneda quizá favorezca al Gobierno de Pekín. Washington siempre ha ido a la vanguardia de la innovación y la aplicación de medios digitales a sus sistemas militares y civiles, y eso también plantea ciertas debilidades. Ya en 1998, dos coroneles chinos, Lian Qiao y Wang Xiangsui, publicaron

un artículo llamado «Guerra ilimitada», en el que destacaban que la excesiva dependencia de Estados Unidos de las tecnologías informáticas aplicadas a la defensa debía ser explotada para conseguir una «ventaja asimétrica».

De este modo, la aparente ventaja de partida con la que contaba Estados Unidos por haber sido el desarrollador de internet es un arma de doble filo, y queda mitigada o neutralizada por los elementos de dependencia tecnológica. Por este motivo, numerosos expertos sostienen que la ciberguerra es «el gran factor nivelador», al no proporcionar automáticamente una ventaja a los países grandes y poderosos sobre los más pequeños. De todos modos, también hay quien pone en cuestión que esto sea así: al fin y al cabo, los recursos importan, y los países que puedan invertir más en innovación digital, en ordenadores y en personal cualificado siempre jugarán con un as en la manga.

Sabiendo esto, China ha comenzado a equiparse para futuras ciberamenazas y conflictos, y el gasto en ciberguerra ha pasado a representar una de sus partidas prioritarias. Además, el país se ha dotado de nuevas unidades militares destinadas a preparar ciberataques contra el enemigo que dependen de la sección del Ejército Popular de Liberación equivalente a la NSA. Se estima que esta división cuenta con unos 130.000 hombres. Por otro lado, se sabe de la existencia de cibercomandos chinos asimilables a los USCYBERCOM, que cuentan con al menos diez subdivisiones implicadas en el «diseño y desarrollo de redes de ordenadores para la defensa, el ataque y los sistemas de explotación».

Cabe citar al segundo departamento del Ejército Popular de Liberación (EPL2) encargado del espionaje exterior y de imágenes; y el EPL3, encargado del espionaje de señales y cibernético.

Pero hay más grupos gubernamentales chinos destinados a labores de ciberguerra. Por ejemplo, el conocido como Shanghai Group, que se centra en tareas de inteligencia económica, política y militar sobre Estados Unidos empleando medios digitales. Este grupo fue el responsable, en el año 2013, del robo de claves de acceso para romper la seguridad de *The New York Times*. Por desgracia para ellos, el *Times* se vengó haciendo una serie de publicaciones

embarazosas para el Gobierno chino. El diario reveló la existencia del Shanghai Group, hasta entonces secreto, y afirmó que estaba detrás de más de 140 ciberataques a industrias y sedes gubernamentales, desde Coca-Cola hasta el Pentágono o las Naciones Unidas. Además, los chinos tuvieron que soportar la humillación de ver cómo la sede del grupo en Shanghái era llevada a la portada del *Times*.

A pesar de estos tropezones, China sigue determinada a hacer de la ciberguerra una de sus prioridades presupuestarias. Pekín considera que la inversión en investigación, desarrollo e innovación (I+D+i) aplicados al espionaje digital y la guerra en internet constituyen una estrategia crucial, y así lo ha hecho constar en su Plan Quinquenal 2011-2015.

La escalada militar en internet, que ya puede considerarse una verdadera carrera de ciberarmamento, ha despertado preocupación internacional. La red, concebida como un espacio democrático único para compartir y comunicarse, se ha transformado en un nuevo campo de batalla. Y eso es peligroso. Puede que el único consuelo que nos quede sea el de confiar, como en tiempos de la guerra fría, en que la disuasión funcione. Como expresó muy bien un oficial de alto rango del ejército chino: «Estados Unidos tiene piedras grandes en sus manos, pero también ventanas de cristal. China tiene piedras grandes en sus manos, pero también ventanas de cristal. Quizá por ello hay cosas en las que podemos ponernos de acuerdo».

## Hackers patrióticos: unos «motivados» del sistema

Buena parte de los muchos ciberprogramas desarrollados por el Gobierno de China se localizan en universidades de ingeniería o compañías tecnológicas. El Ejército Popular de Liberación utiliza las escuelas y las empresas como viveros para la localización de talentos y la formación de personal con el que luego nutrir sus divisiones de ciberguerra. También organiza torneos regionales para identificar a hackers avanzados. Así, ha creado una milicia de «hackers patrióticos» para que sirvan al país en misiones de guerra digital.

Es cierto que, a veces, controlar a estos jóvenes e impetuosos hackers resulta un poco complicado, incluso para el todopoderoso gobierno de China. Por ejemplo, el vencedor de uno de los concursos regionales de *hacking* organizados por el Estado chino tuvo que ser arrestado en 2005 por lanzar ciberataques sobre las webs de hackers rivales.

En otro episodio embarazoso, a punto de celebrarse los Juegos Olímpicos de Pekín 2008, cuando el Gobierno sólo quería buenas noticias que promocionaran la imagen del país, un grupo de hackers patrióticos distribuyó instrucciones en internet para lanzar ataques virtuales contra la cadena de televisión estadounidense CNN. Al parecer, los hackers estaban enfadados con la CNN por un reportaje que había emitido sobre los disturbios en el Tíbet.

Pero, al margen de algunas meteduras de pata, lo cierto es que las milicias patrióticas digitales son muy eficientes, hasta el punto de que Estados Unidos se toma muy en serio su amenaza. Los norteamericanos todavía recuerdan un suceso que tuvo lugar en 2001, y que dio lugar a un enfrentamiento muy áspero con China. Todo empezó con un accidente ocurrido en la isla de Hainan, cuando el piloto de un caza J-8 chino realizó una maniobra de viraje muy cerca de un avión de vigilancia P-3 de los marines estadounidenses, chocando ambos en el aire. El avión chino, más pequeño, se precipitó a tierra y su piloto murió; mientras que el norteamericano tuvo que realizar un aterrizaje de emergencia.

Los gobiernos de los dos países se acusaron mutuamente por la responsabilidad del siniestro y, como represalia, el Partido Comunista

Chino animó a sus ciudadanos a desafiar la seguridad de las webs estadounidenses para mostrar su descontento con lo sucedido. Los disciplinados hackers patrióticos no tardaron en satisfacer las demandas de sus gobernantes, y emprendieron un gran número de ataques contra cientos de web norteamericanas, desde los sitios de simples bibliotecas públicas, hasta la página de la Casa Blanca.

Después de once días de ataques inmisericordes, la administración del recién elegido presidente George W. Bush aceptó enviar una carta de condolencias y pagar a China 34.000 dólares. Con ello, el Gobierno chino dio por cerrado el enfrentamiento y anunció la normalización de las relaciones con Estados Unidos. Sin embargo, como ya hemos señalado, los jóvenes hackers patrióticos son unos muchachos algo revoltosos y difíciles de controlar. Al final, la policía china hubo de realizar varias detenciones de hackers que se negaban a poner fin a los ataques, que en este caso no estaban autorizados.

A raíz de aquello, el Gobierno chino tomó nota del desmadre y decidió convertir los grupos de hackers patrióticos en organizaciones más formales y controlables. Se estima que estos grupos cuentan con alrededor de 200.000 miembros, más o menos el número de habitantes que tiene una ciudad mediana española.

Unos años más tarde, ya en marzo de 2009, un troyano procedente de China, y que pronto sería conocido como Ghostnet, infectó cerca de 1.300 computadoras, entre ordenadores de la OTAN y de embajadas, ministerios y otros servicios de más de cien Estados diferentes. El virus fue descubierto en Canadá.

Y también será Canadá quien, dos años más tarde, en 2011, denuncie haber sido víctima del «mayor ataque» registrado contra servicios oficiales, incluidas agencias del Departamento de Defensa Nacional. Los canadienses volverán a acusar a China de estar detrás de los ciberataques.

El Gobierno de China, por supuesto, negó en todas las ocasiones tener cualquier responsabilidad en las operaciones de *hacking* descritas. En todas ellas se da por hecho, dada la existencia de diversos indicios, que Pekín estaba detrás de los ataques, pero lo cierto es que no hay pruebas concluyentes de ello.

Estados Unidos, por su parte, no cuenta con una milicia de hackers organizada, al menos por el momento. Washington barajó la cuestión hace algunos años, cuando el general Alexander, entonces al mando de la NSA y los USCYBERCOM, habló de la necesidad de mantener un ejército de hackers con capacidades ofensivas para la prosperidad del país. Sin embargo, esta posibilidad quedó en agua de borrajas cuando Michael Hayden, antiguo director de la NSA y la CIA, hizo unas declaraciones, con su prepotente retórica habitual, afirmando que los hackers eran «nihilistas, anarquistas, activistas… la gente de LulzSec o Anonymous son veinteañeros que llevan cinco o seis años sin hablar con el sexo contrario». Aquello no sentó demasiado bien, y, tras el episodio, parecía algo difícil pedir colaboración hasta que se enfriaran un poco esas declaraciones.

Que no dispongan de un ejército de hackers organizado no significa que Estados Unidos no cuente con la colaboración desinteresada de algunos hackers patrióticos. Es el caso de The Jester, un pirata y ciberpatriota estadounidense que ha servido en el ejército, y que ahora se dedica a lanzar ataques digitales contra los enemigos de su país. A día de hoy se desconoce su identidad real, pero The Jester es consciente de que sus actividades son ilegales y de que es posible que alguna vez sea descubierto. En cualquier caso, tampoco es algo que le preocupe en exceso: «Cuando llegue el momento, pagaré por mis transgresiones y cumpliré mi pena», ha afirmado en alguna entrevista.

Éste es el escenario en el que se mueven algunos de estos hackers. Son *celebrities* modernas, seguidas por miles de personas, e inspiran con sus valores a los más jóvenes, que en ocasiones les idolatran, además de gozar de un cierto reconocimiento social, pese a que, con la ley en la mano, sus actividades son delictivas. Me atrevería a decir que algunos son «tontos útiles del sistema». Se los utiliza y lanza contra objetivos, y, como sucedió en China, si los acontecimientos se precipitan, siempre se les puede detener como cabezas de turco para demostrar que se han tomado medidas, y que el atacante no era miembro del sistema.

Alguien como The Jester, que tiene cuenta en Twitter (desde el año 2009) y página web conocida, y que incluso ha llegado a donar

su ordenador portátil, en un curioso caso de fetichismo, al Museo Internacional del Espionaje, ubicado en Washington, no debería ser muy difícil de localizar para el FBI. A no ser que no quieran hacerlo, por supuesto.

La dificultad a la hora de atribuir la autoría de los ciberataques es una constante en internet. Hoy en día, para algunos de los casos de ciberguerra más sonados no existe un culpable identificado. Por ejemplo, en 2013, Corea del Sur sufrió uno de los mayores ciberataques de la historia, en el que más de 30.000 ordenadores de los bancos más importantes del país, así como de cadenas de televisión e instituciones financieras fueron víctima de un virus desconocido. Corea del Sur lanzó acusaciones por lo sucedido tanto a Corea del Norte como a China, pero lo cierto es que, a día de hoy, ninguna de las dos ha podido ser demostrada.

De igual modo, en octubre de 2012 se produjo una cadena de ciberataques que fue bautizada como «Octubre rojo», y cuyos objetivos eran Europa, Asia y América del Norte. Este caso es especialmente relevante, porque el virus en cuestión, además de atacar a agencias gubernamentales y diplomáticas, robaba información sobre infraestructuras críticas, lo cual desató todas las alarmas en los gobiernos de los países afectados. Aunque no ha podido ser confirmado, y en un primer momento se habló de China, expertos en seguridad informática de Kaspersky señalaron que el origen de los ataques podría ser Rusia.

## Desde Rusia, con amor

Efectivamente, China no es el único país que tiene un ejército de hackers a su servicio. Uno de los episodios de ciberguerra más célebres es el que protagonizaron Rusia y Estonia en 2007, con hackers patrióticos rusos como protagonistas. Ese año, las páginas web del pequeño país báltico fueron víctima de una serie de ataques de denegación de servicio. El entonces ministro de Asuntos Exteriores, Urmas Paet, no dudó un segundo a la hora de acusar a un culpable: Rusia. Paet, muy enfadado, acusó al Kremlin de intentar paralizar la economía estonia: «Rusia está atacando a Estonia, y los ataques son virtuales, psicológicos y reales».

La respuesta de los rusos no se hizo esperar, pero, para sorpresa de todos, ni siquiera trataron de disimular su responsabilidad en los ataques. El líder parlamentario Sergei Markov le sugirió a los estonios que no miraran con dudas al Kremlin. «Sobre el ciberataque a Estonia, no busquéis más: el ataque fue llevado a cabo por mi ayudante», declaró. Efectivamente, el joven asistente de Markov no tuvo problema en reconocer su autoría. El muchacho era el líder de Nashi (que puede traducirse como «Lo Nuestro»), un movimiento ruso de 120.000 jóvenes entre diecisiete y veinticinco años que, aunque no pertenece oficialmente al Gobierno, fue organizado por los seguidores de Putin para perseguir las actividades antipatrióticas. Esto implica lanzar ataques informáticos, como en el caso de Estonia, pero sus funciones abarcan un amplio abanico: desde organizar campamentos deportivos de verano, hasta reventar manifestaciones en contra del régimen y agredir a sus asistentes. Angelitos.

Pero ¿cuál es la terrible ofensa en la que había incurrido Estonia para que Rusia mandara a sus milicias hackers atacar las webs del país? Pues que había retirado una estatua, el Soldado de Bronce de Tallin, del monumento conmemorativo de la liberación de Tallin por los soviéticos en la segunda guerra mundial. ¿Exagerado? No para los nacionalistas rusos. Al parecer, para la mayoría de los estonios, la escultura simbolizaba décadas de opresión bajo el yugo imperialista soviético. Sin embargo, para los rusos se trataba de un

reconocimiento al valor y el heroico sacrificio desplegado por el Ejército Rojo contra la Alemania nazi.

Ese mismo año de 2007, Rusia emplearía la fuerza digital para llevar a cabo ataques digitales contra Ucrania. Concretamente, en el mes de octubre, un grupo de hackers nacionalistas teledirigidos por Moscú y pertenecientes al Movimiento de Jóvenes Euroasiáticos se atribuyó el ataque contra la web del entonces presidente ucraniano Viktor Yushchenko.

Y sólo un año después de los ciberataques contra Estonia, durante la breve guerra que enfrentó a Georgia y Rusia en 2008, las milicias de hackers patrióticos volvieron a hacer aparición orquestados por el Gobierno de Moscú. Sincronizaron sus ciberataques con las operaciones militares de las tropas, y tuvieron acceso incluso a listas de objetivos investigados del gobierno georgiano que les suministró presuntamente el Kremlin.

También en 2008, hackers dirigidos por los gobiernos de Rusia y China se infiltraron en los ordenadores del presidente Obama y de su rival republicano en la competición por llegar a la Casa Blanca, el senador McCain. Asimismo, se cree que fue el Gobierno de Pekín el responsable de una infiltración en los ordenadores de Israel en los años 2012 y 2013, con el fin de obtener información sobre su sistema antimisiles conocido como Iron Dome (Cúpula de Hierro).

A pesar del uso ofensivo que el Kremlin hace de internet, Putin es muy consciente de que la red es un arma de doble filo que también se puede volver en su contra. De hecho, él y sus colaboradores están convencidos, no sin cierta razón, de que las «revoluciones de colores» en Ucrania y en otras antiguas repúblicas de la Unión Soviética fueron espoleados por la inestabilidad política promovida a través de internet, por ejemplo, mediante la convocatoria de manifestaciones contra el Gobierno ruso en 2012.

Oriente Medio también ha sido, por su profusión en conflictos, un buen caldo de cultivo para hackers patrióticos. Cuando estalló la guerra civil en Siria, por ejemplo, un colectivo de hackers autodenominados Ejército Electrónico Sirio realizó una serie de ataques contra páginas web que se habían mostrado críticas con el Gobierno del dictador Assad. El presidente dijo entonces que el

grupo era «un ejército electrónico que ha servido como un ejército real en la realidad virtual».

Pero, aunque las milicias de hackers patrióticos sean un instrumento masivo, barato y eficaz en manos de muchos gobiernos y un quebradero de cabeza para países como Estados Unidos, la ciberguerra de los adultos es una cosa mucho más seria y peligrosa. Además, estos grupúsculos de chicos no dejan de ser poco más que los voluntariosos becarios del asunto.

## Bombas digitales, ¿bombas reales?

En el año 2006, un alto funcionario del Gobierno de Siria se encontraba de visita en Inglaterra. Después de dejar sus pertenencias en el hotel, decidió que era un buen momento para salir a hacer turismo por Londres. Todo parecía normal, pero el hombre ha cometido un error incalculable: ha dejado su ordenador en la habitación. Aprovechando su ausencia, un grupo de agentes del Mossad, la agencia de inteligencia de Israel, entrará en su dormitorio con el propósito de instalar un troyano en su portátil, el cual les permitirá después monitorear sus comunicaciones.

Sin embargo, para sorpresa de los propios israelíes, a la hora de acceder al ordenador para infectarlo con el troyano, los agentes encontrarán más información de la que esperaban en el dispositivo del imprudente funcionario sirio. Entre sus archivos hallarán una foto que enseguida llamará poderosamente la atención del Mossad. Se trata de una imagen en la que puede verse a un individuo asiático vestido con un traje azul junto a otro de aspecto árabe, con el desierto sirio como telón de fondo. A los agentes de inteligencia no les costó mucho identificar a ambos hombres como Chon Chibi, director del programa nuclear de Corea del Norte, y Ibrahim Othman, director de la Comisión de la Energía Atómica de Siria. Si una foto vale más que mil palabras, la casualidad les había llevado a dar con el premio gordo de las fotografías. Una pista que evidenciaba muchas cosas.

Además de la sospechosa fotografía, en el ordenador encontraron planos de construcción, así como imágenes de un tipo de tubería utilizada para trabajos con material fisible y otros documentos que hicieron que los israelíes se dieran cuenta del alcance de la información contenida en el portátil. Los sirios estaban creando una infraestructura en Al Kibar para procesar plutonio, un paso clave para después poder desarrollar la bomba nuclear. Todo ello con la ayuda de un enemigo declarado de Occidente como Corea del Norte.

Con los datos intervenidos, Israel puso en marcha la llamada Operación Huerta. Durante la medianoche del 6 de septiembre de

2007, siete cazabombarderos F-151 del ejército israelí cruzaron el espacio aéreo sirio, penetraron en su territorio y lanzaron varias bombas sobre el complejo nuclear de Al Kibar descrito en las fotografías. ¿Lo más sorprendente? Durante todo el tiempo que duró la operación, ni una sola bala fue disparada contra los intrusos israelíes.

¿Cómo es posible que una flotilla de cazabombarderos de una fuerza extranjera pudiera invadir el espacio aéreo de un Estado rival y se fuera de rositas? Muy sencillo: porque los radares y los sistemas de detección aéreos sirios nunca detectaron la intrusión. No fueron conscientes de que estaban siendo víctimas de un ataque hasta que las bombas alcanzaron su objetivo.

El ordenador del funcionario sirio había resultado mucho más útil de lo esperado. Lo habían intervenido con el objetivo de inocularle un virus que permitiera intervenir sus comunicaciones, pero, de repente, se dieron cuenta de que podían obtener mucho más que eso de él. Podían penetrar en las redes de ordenadores del ejército sirio y ver todo lo que los sirios estaban haciendo en cada momento. De este modo, sustituyeron las imágenes de los radares por otras falsas, de tal modo que los vigilantes no pudieran ver en tiempo real el ataque israelí. Mientras los sistemas de defensa sirios recibían imágenes de absoluta normalidad, los bombarderos israelíes estaban destruyendo todo el complejo que albergaba el programa nuclear del dictador Assad. La operación fue un éxito, y los israelíes lograron su objetivo sin lamentar ninguna pérdida, y con una inferioridad de fuerzas notable. Esta acción demuestra lo intrépidas y brillantes que son las fuerzas de Israel.

La acción emprendida por los servicios de inteligencia de Israel sirve para ilustrar muy claramente el nuevo papel de las armas digitales en la guerra convencional. Por poner un ejemplo, si en los conflictos tradicionales las agencias de espionaje de los Estados eran capaces de interceptar y descifrar las señales de radio del enemigo, en la ciberguerra, los servicios secretos pueden tomar el control de las mismas, literalmente.

La dependencia de lo que muestran las pantallas hace que, si éstas fallan, estemos a ciegas. Más que nunca, parafraseando a

Groucho Marx, se les podría haber dicho a los controladores sirios, mientras les llovían misiles y sus pantallas de radar mostraban una noche tranquila: «¿A quién va usted a creer, a mí o a sus propios ojos?».

## Hay un gusano en mi manzana

No es casualidad que fuera precisamente Israel el país que llevara a cabo una operación de estas características contra Siria. El Estado judío es una de las mayores ciberpotencias, y no en vano destina una partida de gasto muy elevada a labores de innovación tecnológica aplicada a la inteligencia militar. No es para menos. Para los israelíes se trata de una cuestión de supervivencia, habida cuenta de que la mayor parte de los países con los que comparte región geográfica sueñan con destruirlos.

Pero Israel no es el único Estado que tiene enemigos en Oriente Próximo y Oriente Medio.

En el año 2010, los expertos en seguridad digital entraron en pánico con la aparición de una nueva modalidad de virus informático. Un tipo de gusano mucho más sofisticado y peligroso de lo que el mundo había conocido hasta la fecha. Lo bautizaron Stuxnet, y está considerado como la primera arma de guerra digital a gran escala. Casi podríamos denominarlo como un arma de destrucción masiva digital. Stuxnet es el rostro de la guerra del siglo XXI: invisible, anónimo y devastador.

Era una noche calurosa de julio, cuando decenas de teléfonos móviles comenzaron a sonar por toda Europa. Sus propietarios buscaron a tientas los *smartphones* en la mesilla y descolgaron entre bostezos. Sentados en el borde de la cama, aún con los ojos pegados, escucharon las instrucciones de un mando de la OTAN al otro lado de la línea: acababan de llamarles a filas. En los días sucesivos, nuevos reclutas se sumaron a los recién movilizados soldados, pero, esta vez, los incorporados compartían una característica poco habitual que les hacía especiales: eran analistas de *software* o expertos en sistemas de control industrial.

Un virus informático con capacidad para autorreplicarse, un gusano, estaba infectando miles de ordenadores en todo el mundo. El virus buscaba unas pequeñas cajas de plástico gris llamadas controladores lógico-programables, del tamaño de un paquete de lápices de colores, y se introducía en ellos. Estos controladores, también llamados PLC, son los que regulan la maquinaria en las

fábricas, las centrales eléctricas y los proyectos de construcción e ingeniería. Los PLC realizan el trabajo sucio más crítico de la vida moderna: abren y cierran las válvulas en las tuberías de agua, aceleran y frenan el giro de las centrifugadoras de uranio, dosifican la cantidad de crema en cada galleta Oreo (esto es lo realmente trascendente) y calculan el momento en que los semáforos deben cambiar de rojo a verde. Huelga decir que un fallo de estos sistemas puede tener consecuencias catastróficas. ¡Sobre todo en el caso de las Oreo!

Los controladores PLC están por todas partes. Sin embargo, casi nadie sabe cómo funcionan. De hecho, cuando estalló la crisis Stuxnet, la mayoría de los altos funcionarios de los gobiernos amenazados por el virus ni siquiera conocían la existencia de los PLC. El desconocimiento sobre el problema era generalizado, y los poderes occidentales comenzaron a creer que la función del virus era acometer un ataque generalizado contra los PLC. Si esto era así, eso significaba que las fábricas dejarían de funcionar y las centrales eléctricas se apagarían irremediablemente en todo el mundo. En estas circunstancias, se preguntaban ¿cuánto tiempo podrían garantizar el orden social? ¿Quién podría haber desarrollado semejante arma? Y, sobre todo, ¿para qué?

Afortunadamente, las luces todavía funcionaban, así que los expertos se centraron en tratar de averiguar qué rayos quería Stuxnet. Al escuadrón de *geeks* de los gobiernos se unió una pequeña milicia ciudadana de analistas aficionados y profesionales repartidos en varios continentes, después de que el código del gusano fuera hecho público en internet.

Stuxnet era la mayor muestra de *software* malicioso que la mayoría de los investigadores había visto nunca, y tenía la estructura más compleja conocida en un virus. Para que te hagas una idea, el gusano Conficker, que hasta la fecha estaba considerado el «campeón de los pesos pesados» de los gusanos, tenía sólo una vigésima parte del tamaño de esta nueva amenaza. A lo largo de los meses posteriores, un puñado de analistas obcecados logró descifrar finalmente casi todo el programa, y lo que contemplaron ante sus ojos les pareció el mismo infierno.

## Tres, dos, uno..., *zero days*

Para infectar los ordenadores, Stuxnet aprovechaba vulnerabilidades no conocidas de Windows. Estas puertas, llamadas *zero days* (o «días cero»), son muy difíciles de descubrir, tanto que pueden alcanzar un valor de más de 100.000 dólares en el mercado negro. Son tan valiosas que los hackers que las encuentran se cuidan mucho de no hacerlas públicas. Si descubres un *zero*, felicidades, te acaba de tocar la lotería, y, si lo colocas bien, ganarás mucho dinero. Por eso había algo que no encajaba con Stuxnet. El virus no sólo era sorprendente por utilizar una vulnerabilidad del sistema desconocida hasta la fecha, sino que empleaba hasta cuatro *zero days*, algo sin precedentes. A priori, esto no tenía mucho sentido: ¿para qué desvelar la existencia de cuatro puertas traseras cuando con una habría sido suficiente? ¿Qué tipo de hacker es capaz de descubrir cuatro *zero days* para después hacerlos públicos sin más?

Parecía evidente que, fuera quien fuera el diseñador del virus, tenía muchos recursos y quería asegurarse de que el gusano penetrara en su objetivo. Stuxnet atacaba los ordenadores de dos formas simultáneas. Primero instalaba un programa que permitía al virus hacer lo que quisiera con el ordenador, y después inoculaba una carga maliciosa tan endiabladamente encriptada que resultaba inescrutable. Además, tal como explicó el periodista Michael Joseph Gross, «el gusano utilizaba una firma digital, una cadena cifrada de bits que los programas de *software* legítimos llevan para mostrar que vienen en son de paz. Las firmas digitales son como pasaportes para el *software*: una prueba de identidad para los programas que cruzan la frontera entre una máquina y otra. A veces, los virus utilizan firmas digitales falsificadas para obtener acceso a las computadoras, como adolescentes que usan identificaciones falsas para entrar en los bares. Los analistas de seguridad llevaban varios años esperando que los creadores de *malware* dieran el salto de las firmas falsificadas a las firmas genuinas robadas. Y ésta fue la primera vez que se tuvo constancia de que había sucedido».

Otro dato curioso sobre Stuxnet es que había sido detectado sólo en unos pocos lugares de Europa y Estados Unidos. El mayor

número de infecciones, con diferencia, se había producido en Asia, donde ya había más de 15.000 casos y la cifra iba en aumento. Los países más afectados por el gusano eran India, Indonesia y, significativamente, Irán.

Finalmente, tras un proceso arduo, los expertos llegaron a la conclusión de que el objetivo de Stuxnet era, efectivamente, los controladores PLC. Eugene Kaspersky, director de una de las empresas de seguridad informática más importantes del mundo, comenzó a sospechar que Stuxnet debía de ser obra de algún Gobierno. Consideraba que habría requerido demasiado tiempo localizar todos los defectos de los cuatro *zero days* sin tener acceso al código fuente de Windows, y que habría resultado demasiado complejo para un *outsider*. Al darse cuenta de esto, Kaspersky llegó a afirmar: «Estamos entrando en una zona muy peligrosa. El siguiente paso, si queremos seguir por este camino, es pensar que hubo una llamada de Washington a Seattle para ayudar con el código fuente». Efectivamente, se hace dificilillo pensar que un Gobierno que no fuera el estadounidense pudiera haber llamado a Bill Gates para que solucionara los detallitos de un acceso rápido al código fuente de Windows.

La cosa se pone fea. Los expertos están perplejos con el grado de complejidad de Stuxnet y, estudiando su código, estiman que en él debieron de trabajar alrededor de treinta personas (los estilos de programación son diferenciables, del mismo modo que lo es la prosa de los escritores). Además, calculan que deben de haberse empleado seis meses de trabajo para poder desarrollar completamente el gusano.

Finalmente, será Ralph Langner, un experto alemán en seguridad informática, quien dará con las claves de Stuxnet. Langner descubrirá que el virus no sólo se dirige contra los controladores PLC, sino que tiene preferencia por un fabricante determinado: los sistemas de Siemens. Además, descubrirá el modo en que opera el gusano: cuando Stuxnet infecta un ordenador, intenta propagarse a todas las computadoras de la red a la que está conectado ese equipo y trata de averiguar si alguno está ejecutando el *software* de Siemens. Si la respuesta es no, Stuxnet se convierte en una función

inútil, inerte en la red. Si la respuesta es sí, el gusano comprueba si el ordenador está conectado a un PLC o espera hasta que lo haga. Después busca un determinado tipo de maquinaria en el PLC. Si Stuxnet encuentra la pieza de maquinaria que está buscando, comprueba si ese componente está operando bajo ciertas condiciones. Si es así, Stuxnet inyecta su propio código malicioso en el controlador para cambiar la forma en que la maquinaria funciona. Por último, «engaña» al sistema de seguridad digital de la máquina para hacerle creer que todo funciona con normalidad.

## La respuesta está… ¡en la Biblia!

Se habían dado muchos pasos para desentrañar el misterio de Stuxnet, pero aún quedaban los dos mayores enigmas por ser resueltos: ¿contra quién iba dirigido Stuxnet? y ¿quién era su creador?

Una de las cosas que más había llamado la atención de los expertos que habían trabajado descifrando el código del virus era la siguiente secuencia: b:\myrtus\src\objfre*w2k*x86\i386\guava.pdb.

Aquella referencia a Myrtus les condujo al libro bíblico de Ester, una historia en la que se narra cómo los judíos arruinan un complot de los persas contra su pueblo. Aquello empezaba a sonar sospechoso.

Langner sabía que el gusano perseguía un controlador industrial muy concreto, manufacturado por Siemens y configurado para ejecutar una serie de centrifugadoras nucleares, pero no unas centrifugadoras cualesquiera, sino una serie de un cierto número de centrifugadoras unidas (984 para ser exactos) y de un tamaño determinado. Casualmente, 984 era el número exacto de centrifugadoras que tenía la planta nuclear de Natanz, una central iraní en la que se sospechaba que podían estar siendo desarrolladas ilegalmente armas nucleares.

Además, se averiguó que el virus atacaba las centrales de dos maneras: en primer lugar, era capaz de alterar la velocidad de centrifugado, lo cual puede dañar o destruir las máquinas. Por otro lado, el gusano ocultaba su actividad para que no pudiera ser detectado. Los sistemas de control industriales habían sido víctimas de sabotajes en otras ocasiones, pero nunca habían podido ser programados de forma remota sin que nadie tuviera que pulsar algún botón en alguna parte, como hacía Stuxnet. Este nuevo gusano era como un dron sigiloso y autodirigido, el primer virus conocido que, una vez liberado, busca un objetivo específico, lo sabotea y después oculta su propia existencia y sus efectos hasta que el daño ya está hecho. En resumidas cuentas: Stuxnet era diabólicamente genial.

Langner sabía que el objetivo de Stuxnet era arruinar el programa nuclear iraní, y tenía pocas dudas de que la mano de Israel estaba detrás de lo sucedido. Había resuelto el puzle. Después se confirmó que, efectivamente, Stuxnet era un proyecto desarrollado por el Mossad en colaboración con Estados Unidos.

Desde luego, ésta no era la única técnica utilizada por los israelíes y los norteamericanos para frenar el programa de proliferación nuclear de Irán. Una vez la vía diplomática estuvo agotada, y se hubo comprobado que los embargos y bloqueos económicos no conseguían convencer a Irán de poner fin al enriquecimiento de uranio con fines armamentísticos, Israel y Estados Unidos decidieron que había llegado el momento de continuar la política por otros medios, es decir, de ir a la guerra.

Stuxnet forma parte de la vía militar emprendida contra el Gobierno de Teherán, pero no es la única acción llevada a cabo, ni internet el único medio empleado. La operación Juegos Olímpicos (así se llamó) en la que se circunscribe el proyecto Stuxnet fue ideada por la administración Bush y continuada durante la presidencia de Obama, pero la ciberguerra contra Irán ha ido acompañada de intervenciones militares convencionales, como la que acabó con la vida de uno de los científicos nucleares de Teherán y trató de liquidar a otro físico más.

Comprobamos cómo la ciberguerra no está aquí para sustituir a la guerra tradicional, sino para complementarla. La ciberguerra sólo introduce un campo de batalla nuevo, pero no pone fin a los campos de batalla clásicos. Eso sí, internet no es un campo de batalla cualquiera.

Algunos expertos consideran que los ciberataques pueden reducir la violencia mundial existente al permitir a los Estados y a los individuos alcanzar sus objetivos políticos sin tener que recurrir a la violencia física. Desde ese punto de vista, la escalada armamentística en la red puede considerarse como parte lógica de la evolución de la humanidad, un síntoma de modernización. Ésta es una teoría curiosa, pero no carente de cierto sentido. No sé si Stuxnet impidió una guerra, pero, desde luego, sí que evitó una

invasión, y hasta un bombardeo de la central nuclear de Irán. Indirectamente es muy probable que este *software* haya salvado algunas vidas.

No obstante, no todos los expertos son tan optimistas respecto al futuro de la guerra. Como observó Kaspersky sobre el precedente de Stuxnet, virus como éste constituyen «un prototipo funcional y aterrador de un arma cibernética que conducirá a la creación de una nueva carrera armamentística mundial».

Y, como observó Gross: «Stuxnet es el Hiroshima de la ciberguerra. Esto es muy significativo, y la especulación sobre su objetivo y su origen no debería impedirnos ver la cruda realidad. Hemos cruzado una frontera, y ya no hay vuelta atrás».

## El país de Anacleto, agente secreto, y la ciberguerra

En un mundo política, tecnológica y económicamente tan integrado como en el que vivimos, ningún Estado queda al margen de los conflictos en la red, ni siquiera un país de segundo orden como España.

Hace algunos años, un nuevo virus fue introducido en miles de ordenadores en varios países de interés estratégico para España. El troyano en cuestión fue bautizado como Careto, y algunos pasajes de su código malicioso estaban escritos en un español sospechosamente castizo.

A partir de 2007 y hasta principios de 2014, Careto se infiltró en móviles y ordenadores de la administración marroquí; también en instituciones de Brasil, el país extranjero donde hay más inversión empresarial española; mientras que, en España, el País Vasco fue una de sus prioridades, a juzgar por la proporción de pinchazos en la red de Euskaltel, el operador vasco de telecomunicaciones.

Hasta que, en febrero de 2014, la conocida empresa rusa de seguridad informática Kaspersky descubrió el troyano, que fue por primera vez descrito durante una conferencia en la República Dominicana. Una vez fue hecho público en la web de la empresa, el virus Careto no tardó en autoeliminarse de todos los ordenadores que había infectado.

Lo cierto es que el descubrimiento de Kaspersky se produjo casi por casualidad, y fue motivado por un error cometido por los hackers que lo habían diseñado. Al parecer, los desarrolladores del troyano habían tratado de manipular una versión anticuada de un antivirus de la compañía rusa, lo cual llamó la atención de los responsables de la empresa: ¿por qué trataban de manipular una versión antigua en lugar de una actualizada?

Como ha destacado Carlos Barbudo, investigador sobre privacidad y desarrollo de las nuevas tecnologías de la Universidad Complutense de Madrid, Careto «no es un troyano al uso como los utilizados por los cibercriminales. Sus capacidades eran asombrosas, desde robar las pulsaciones del teclado hasta escuchar las conversaciones vía Skype**,** pasando por apoderarse de ficheros».

Además, según se afirmaba en el informe que dio a conocer el nuevo virus, en Careto «observamos un muy alto nivel de profesionalidad».

También Sergio de los Santos, director del laboratorio de Eleven Path, la empresa de ciberseguridad de la multinacional española Telefónica, se sumó a los pareceres de Kaspersky: «Careto alcanzó un elevado nivel de sofisticación, aunque no tanto como Stuxnet».

Pero ¿cómo operaba Careto? El truco era el siguiente. El objetivo recibía un correo electrónico que contenía supuestamente una serie de enlaces a periódicos españoles (sobre todo a *El País* y *Público*) o anglosajones (*The Guardian* era el más utilizado). En realidad, los vínculos tenían trampa. Los destinatarios creían conocer al remitente y pinchaban ingenuamente en los enlaces. Una vez visitaban la web, eran redirigidos a una página que contenía el troyano, y su ordenador quedaba infectado.

## Me cago en la mar

Los expertos estaban de acuerdo en que detrás de un virus de esta complejidad debía de encontrarse un Estado. Se trataba de un programa que buscaba, por ejemplo, la clave de un sistema criptográfico militar o gubernamental, y eso sólo lo puede hacer un Estado. «Nadie invierte tanto esfuerzo y dinero en crear un programa espía si no espera recuperar la inversión con la información obtenida», aseguró por su parte De los Santos.

Efectivamente**,** había algunas evidencias que hacían sospechar del origen español del troyano. Para empezar, vayamos con la más lamentable y divertida. Varias cadenas de texto estaban escritas incorrectamente en inglés (*attempt to move the uploaded file to it's new place*, en lugar de *attempt to move the uploaded file to its new location*) lo cual hacía pensar que ésa no era la lengua materna de los autores del virus Careto. Vamos, que parecía español traducido al inglés.

Por otro lado, algunas cadenas estaban escritas en español, esta vez no sólo redactadas de forma correcta, sino, además, con algunas partes del código escritas en un español muy castizo. Por ejemplo, «mecagoen1mar» era una de las contraseñas que se utilizaban para cifrar las comunicaciones. Y, además, algunas de las carpetas del programa fueron bautizadas con nombres en español, como «Pruebas».

Aparte de estos indicios, Vicente Díaz, analistas e investigadores aseguran que una de las mejores maneras de poder atribuir el origen de un ataque digital es «por el área de influencia», es decir, analizando los lugares donde se ha expandido el virus. Estudiando los objetivos de un troyano resulta más fácil hacerse una idea de qué país podría estar detrás del ciberataque. En este caso, todos los países donde se habían registrado infecciones por el virus Careto se correspondían con Estados en los que España tenía intereses estratégicos.

La gran mayoría de los dispositivos infectados por Careto eran teléfonos móviles y, de ellos, la mayor parte se infectaron en Marruecos. Además, había otros indicios que hacían sospechar de la

autoría de España, como el hecho de que fueran atacados varios ordenadores del País Vasco y, al menos, dos de Gibraltar. Parece evidente que Careto fue una ciberarma desarrollada por España, aunque a algunos expertos les cueste creerlo. Guillem Colom, director del *think tank* Thiber, especializado en ciberseguridad, manifestó serias dudas «de que un producto tan sofisticado sea español, pero si lo fuera sería un hito de la tecnología *made in Spain*».

Lo cierto es que Careto fue, efectivamente, una muestra quizá poco habitual de un producto tecnológico español de gran altura. Era tan preciso que, en sus siete años de vida, sólo infectó a unos pocos miles de ordenadores, lo cual le permitía continuar operando sin despertar demasiadas sospechas. No como otros troyanos, como Downadup o Bugbear, que en su momento afectaron a millones de ordenadores. Los equipos infectados, según explicó Kaspersky, se conectaban únicamente a través de 909 direcciones de IP, el 42 por ciento de ellas, marroquíes. El año de mayor actividad fue 2012.

Una vez el foco puesto en España, parece que la única agencia capaz de llevar a cabo un proyecto de *software* de este tipo, con los recursos humanos y económicos que requiere, sería el Centro Nacional de Inteligencia (CNI).

Sobre los objetivos contra los que se dirigía Careto no se saben muchos más detalles. La política de la empresa que lo descubrió es firme en este sentido, y sólo comparte esta información con las fuerzas de seguridad de los países donde están los equipos infectados.

## *C'est la guerre!*

Pero, en la guerra, no todo son tareas ofensivas, y nunca hay que descuidar la defensa. Igual que parece que podemos atribuir ciertos éxitos a nuestro país, España también ha sido víctima de ataques digitales dirigidos por otros Estados, y quizá el más sonado de ellos fuera el virus Babar, con origen en Francia.

El troyano fue dirigido contra España en los momentos más duros de la crisis económica, cuando Francia quiso saber qué decisiones pensaba tomar el ejecutivo español, entonces presidido por José Luis Rodríguez Zapatero.

Su existencia, sin embargo, no fue conocida hasta varios años más tarde, cuando fue revelada por el diario francés *Le Monde*, después de que Snowden entregara a dicho periódico un documento en el que aportaba pruebas de la existencia de Babar, así como de su origen y sus objetivos.

Los documentos filtrados procedían de la agencia de contraespionaje canadiense, el Centro de Seguridad de las Telecomunicaciones de Canadá (CSTC), que en uno de sus informes señalaba: «En un momento en que España era el centro de atención, porque podía arrastrar a la zona del euro hacia el abismo, se trataba de saber qué medidas barajaba tomar su ejecutivo y en qué plazos para enderezar la situación».

Además, la agencia añadía: «Estimamos, con un nivel moderado de certeza, que se trata de una operación en las redes informáticas respaldada por un Estado y ejecutada por una agencia francesa de inteligencia».

También los otros cuatro integrantes de la alianza Five Eyes (Estados Unidos, Reino Unido, Australia y Nueva Zelanda) estuvieron de acuerdo con el diagnóstico canadiense. Además, explicaron que el objetivo original para el que se diseñó Babar era el mismo que el de Stuxnet: Irán. El troyano se introdujo en los ordenadores de media docena de instituciones iraníes vinculadas al programa nuclear, entre ellas, tres universidades y la Organización de Energía Atómica de Irán (OEAI). Sin embargo, posteriormente, y a tenor de los buenos rendimientos que había tenido el virus, Francia decidió emplearlo para otras labores de espionaje y ciberguerra. En concreto, Babar fue usado para espiar al menos a cuatro países amigos (España, Canadá, Noruega y Grecia) y a dos países africanos (Argelia y Costa de Marfil).

El informe de la agencia de contraespionaje canadiense no revelaba el número de ordenadores que habían resultado infectados, ni cuáles eran sus objetivos concretos, pero resulta bastante

iluminador y aleccionador respecto a algo: en el mundo moderno uno no puede fiarse ni de sus aliados, por mucho que sean sus vecinos.

## Una nueva carrera de armamentos

Recordemos una lección de historia fundamental. En junio de 1946, Bernard Baruch, quien fuera representante personal del entonces presidente Harry S. Truman, pronunció el siguiente discurso ante las Naciones Unidas: «Estamos aquí para elegir entre estar entre los vivos o los muertos… Si fracasamos, habremos condenado a todo ser humano a ser esclavo del miedo. No nos engañemos, hemos de elegir entre paz o destrucción mundial».

En aquella fecha, Estados Unidos era el único país del mundo que había conseguido desarrollar la bomba atómica. El ofrecimiento que Baruch hizo ante la ONU fue muy claro, y hoy apenas nadie lo recuerda: su país se ofrecía a entregar todas sus bombas atómicas a la organización, a cambio de que el resto de países se comprometiera firmemente a no proliferar nuevo armamento nuclear y abriera sus puertas para facilitar las inspecciones necesarias para comprobarlo.

En aquel momento, la Unión Soviética estaba muy lejos de alcanzar el objetivo nuclear (le costaría tres años más conseguir desarrollar la bomba atómica), pero su respuesta a Baruch fue tajante: No. Rusia no se fiaba de los norteamericanos, y también desconfiaba de la ONU, porque consideraba que Estados Unidos tenía mucho poder dentro de la organización, así que estableció nuevas condiciones para el acuerdo: Estados Unidos entregaría su armamento nuclear, y sólo después, se procedería a desarrollar un sistema internacional para el control de la proliferación nuclear.

Lo que siguió luego es por todos conocido: no hubo acuerdo. El plan Baruch fracasó, dando el pistoletazo de salida a la carrera de armamento que marcaría la guerra fría. Te daré sólo un dato para que te hagas una idea de la magnitud de la escalada: en los cincuenta años siguientes, se fabricarían más de cien mil bombas atómicas, con el consiguiente riesgo de destrucción del planeta. Es escalofriante pensarlo, pero, afortunadamente, el mundo sobrevivió y dejó atrás esa funesta etapa.

¿La dejó atrás? Bueno, puede que no del todo. Según expertos en seguridad, actualmente estamos entrando en un nuevo periodo

de carrera armamentística. Los países estarían cometiendo el mismo error que en los años cuarenta al no poner control sobre la proliferación de armas digitales (basta decir que cada segundo se desarrollan nueve programas informáticos maliciosos nuevos), y esto podría tener consecuencias devastadoras.

Para muestra de esta nueva escalada armamentística, un botón: el ejército estadounidense prevé sustituir el 20 por ciento de sus soldados por robots de aquí a 2021. Rusia trabaja en hacer lo mismo. Y es que la tecnología lo está cambiando todo, pero, a su vez, nos hace más dependientes de ella. Es paradójico, pero real. Si bien podemos asegurar que ningún niño nacido hoy necesitará aprender a conducir, y esto es un evidente avance para la sociedad, también eso nos hará más dependientes y vulnerables ante esas tecnologías.

Nuestros hijos, dentro de veinte años, convivirán con robots domésticos que les enseñarán a hablar, andar y realizar diversas tareas, pero estas máquinas generarán una dependencia y un riesgo en sí mismas para todos nosotros.

## El fantasma de la guerra fría

En cualquier caso, existen algunas diferencias entre la carrera de armamentos de la guerra fría y esta digital del siglo XXI, y la principal de ellas tiene que ver con el número de actores implicados, mucho mayor en esta segunda escalada. Ya hay más de cien países que están acumulando potencial cibermilitar. Y con esto no nos referimos únicamente a construir defensas electrónicas, sino también a desarrollar nuevas armas ofensivas.

No obstante, según la empresa californiana de seguridad informática McAfee, se calcula que sólo una veintena de países cuenta con «programas avanzados de ciberguerra» capaces de desarrollar virus comparables a Stuxnet; y, de ellos, sólo un puñado es capaz de llevar a cabo «ciberataques prolongados y sofisticados».

La paradoja que plantean las carreras de armamentos es que ellas mismas se retroalimentan, pues, como una pescadilla que se muerde la cola, «cuanto más rivalizan los Estados en acrecentar su potencial, menos seguros se sienten». Estados Unidos y China están llevando a cabo un esfuerzo militar muy importante para dotarse de armas en el ciberespacio, sin embargo, cuanto más lo hacen, más crece la amenaza recíproca que el uno representa para el otro.

Otra de las características de esta nueva carrera de armamentos es que el uso de las nuevas armas da lugar a una rápida propagación de las mismas, poniendo fin enseguida a la ventaja competitiva que el desarrollador tenía antes de lanzarla. Mientras que los secretos de fabricación de una bomba atómica no son revelados con su detonación, los de un arma digital como Stuxnet sí, ya que su código es puesto al descubierto tan pronto como se libera en la red. De este modo, si el Stuxnet original requirió grandes esfuerzos de investigación y de equipo humano, una vez fue utilizado, cualquiera con los conocimientos técnicos suficientes pudo copiarlo empleando muchos menos recursos y tiempo.

Esto es lo que ha hecho posible que cientos de potenciales atacantes puedan desarrollar gusanos similares a Stuxnet. Si antes de la liberación del virus sólo un reducido grupo de unas cinco personas en el mundo era capaz de desarrollar algo parecido, tras su

uso contra Irán estarían en disposición de crear un gusano semejante varios miles de personas, y ese número crece cada día que pasa. El liberar y utilizar Stuxnet ha sido tremendamente efectivo para estadounidenses e israelíes, pero, en paralelo, ha supuesto dotar de esta arma, y de la capacidad para fabricar sucedáneos, a multitud de países que jamás hubieran podido desarrollarla de otro modo. Esto es un hecho absurdamente similar al que habría ocurrido si, al tirar la bomba atómica, se hubieran lanzado con ella los planos necesarios para su fabricación y replicación inmediata.

Además, los periodos iniciales de una carrera de armamento son los más peligrosos, porque quienes se hallan en posesión de una nueva arma cuentan con incentivos para usarla (de otro modo, su ventaja contra el enemigo desaparecería), pero, al mismo tiempo, se desconocen los efectos que el uso de esa nueva arma puede acarrear.

Por último, en algunas ocasiones, la carrera armamentística puede dar lugar a situaciones verdaderamente surrealistas. Una de ellas tuvo lugar en 1957, cuando los soviéticos lanzaron al espacio el satélite artificial Sputnik, el primero de la historia. La exhibición de poderío militar causó tanto nerviosismo en Washington que la Fuerza Aérea de Estados Unidos llegó a proponer algo tan descabellado como el lanzamiento de un misil nuclear a la Luna, sólo para demostrar que su país también tenía una capacidad militar espectacular en el espacio. Gracias a Dios, esa estúpida idea, posiblemente gestada en un ambiente etílico por un grupo de militares con exceso de testosterona, fue desechada. Aun así, da pavor pensar que este tipo de actuaciones erráticas y absurdas pueda contagiarse al ciberespacio.

Es fácil caer en la comparación de la situación actual en el ciberespacio con el precedente de la carrera armamentística nuclear. Después de todo, la destrucción que son capaces de ocasionar las nuevas armas digitales es mayor que la que puede originar cualquier otra arma conocida, a excepción de las armas nucleares.

Sin embargo, hay expertos como Scott Borg, director del instituto independiente Unidad de Ciberconsecuencias de Estados Unidos

(United States Cyber Consequences Unit, US-CCU), que considera que la carrera de armamentos digital no puede compararse con la escalada nuclear de la guerra fría. Y no lo dice con optimismo precisamente.

Borg asegura que «los ataques informáticos podrían destruir generadores eléctricos, incendiar refinerías de petróleo, hacer explotar oleoductos, contaminar el agua potable, provocar fugas de gases tóxicos, dar lugar a accidentes de trenes y aviones, paralizar los servicios de emergencia o reducir al caos el sistema bancario. Y todo sin necesidad de una participación humana directa».

Especialmente crítico resulta el mantenimiento de la electricidad, de la cual dependen todas las infraestructuras humanas, incluyendo las digitales. Un ciberataque que propiciara un apagón generalizado tendría consecuencias incalculables, tanto en términos de desórdenes sociales (los saqueos comienzan, de media, dos horas después de que se produzca un gran apagón) como por sus costes económicos.

Pero, a pesar de su potencial capacidad destructiva, que Borg cree que no tiene precedentes en la historia, el experto considera que no se dan las condiciones para trazar un paralelismo entre la carrera de armamentos de la guerra fría y la actual, y lo cree por diversas razones. «En la época nuclear, las armas más peligrosas exigían vastos recursos. Producir armas nucleares resultaba extremadamente difícil. Muy pocas personas sabían cómo fabricarlas», señala Borg. Además, cada una de las etapas de fabricación, incluyendo las pruebas nucleares, eran muy peligrosas y exigían precauciones especiales. Por no decir que producir armas nucleares era muy caro, se requerían cientos de miles de personas para participar en el proyecto, y el proceso llevaba varios años. Y añade más: «Las armas cibernéticas, en cambio, sólo necesitan recursos modestos» (apenas se necesitan instalaciones físicas para producirlas y su manejo es completamente seguro); y «un equipo de menos de un centenar de personas muy cualificadas lograría crear una devastadora gama de armas en sólo dos o tres años. Varios centenares de personas podrían producir un arsenal de ciberarmas extremadamente destructivas en cuestión de meses» (todo ello con

una inversión presupuestaria mucho más pequeña que la necesaria para proliferar armamento nuclear).

Por otro lado, durante la guerra fría, las armas nucleares estaban únicamente en posesión de los gobiernos de los Estados, mientras que ahora no hay forma de controlar la limitación de ciberarmas, ya que cualquiera puede desarrollarlas o comprarlas.

Añade Borg que, en la actualidad, no existe una definición clara sobre el uso de las armas digitales, como sí había en la guerra fría. Antes, «un país poseía o no armas nucleares. Había una diferencia clara entre hacer explotar un arma nuclear y no hacerlo». Ahora esto es mucho más complicado.

Además, las armas nucleares podían almacenarse, algo que no es posible con las armas digitales, que, si no se usan, muy pronto quedan obsoletas debido a la permanente actualización de las redes informáticas para las que han sido diseñadas.

Las armas informáticas se replican ilimitadamente, se pueden conseguir por dinero y almacenar sin problemas en cualquier sitio. Además, no generan las dependencias y trazabilidad de las armas tradicionales.

Un ataque con este tipo de ciberarmas puede significar poner a tus enemigos al frente de tus instalaciones críticas, o permitirles tomar el control de las mismas.

Asimismo, también han desaparecido en la actualidad las limitaciones geográficas de la guerra, y el principio de disuasión por miedo a la represalia que marcó la guerra fría ha perdido sentido en el nuevo contexto digital, donde los ataques se pueden realizar de forma anónima.

Por último, Borg señala algo que veremos a continuación, y es que, en la era de internet, resulta muy complicado establecer tratados internacionales para el empleo de armas digitales.

## *Inter arma, silent leges*

Que el ciberconflicto no tiene vuelta atrás es algo que ya aceptan todos los gobiernos. La asunción de esta realidad ha dado pie a

nuevos interrogantes. Si la guerra en el ciberespacio ha llegado para sumarse a la guerra convencional, tiene que haber leyes y tratados internacionales que la regulen. O, al menos, debería haberlas. Pero ¿hasta qué punto tiene encaje la ciberguerra en el ordenamiento clásico de la guerra?

Tras los ciberataques de Rusia contra Estonia ocurridos en 2007 por la retirada de la estatua conmemorativa soviética, la OTAN decidió crear la organización Centro de Excelencia de Ciberdefensa, con base en Tallin, la capital de la república báltica. El proyecto reunió a juristas internacionales de prestigio con el objetivo de estudiar la aplicación de las normas legales tradicionales a los casos de conflictos cibernéticos.

De aquellas reuniones, dirigidas por Michael Schmitt, de la Escuela de Guerra Naval (Naval War College) estadounidense, en Bristol (Rhode Island), nació el conocido como «Manual de Tallin», cuyo nombre completo es «Manual de derecho internacional aplicable al conflicto cibernético». Se trata del primer protocolo que intenta arrojar luz sobre el inextricable universo de la guerra en internet, y establece, entre otras cosas, una serie de criterios para dictaminar si un ataque digital constituye o no un uso de fuerza armada susceptible de ser interpretado como *casus belli*.

A pesar del esfuerzo notable realizado por los impulsores del Manual de Tallin, lo cierto es que resulta verdaderamente arduo encontrar un encaje para la ciberguerra en los tratados militares clásicos. El derecho a la guerra, el *ius ad bellum*, continúa rigiéndose por la Carta de las Naciones Unidas firmada al final de la segunda guerra mundial, y huelga decir que, en los años cuarenta, los ciberataques no estaban a la orden del día.

El artículo 2.4 de la Carta establece taxativamente la prohibición del uso de la fuerza contra la independencia política o la integridad territorial de cualquier país. Y no sólo prohíbe el uso de la fuerza, sino también la amenaza. ¿Significa eso que la guerra es ilegal? No exactamente. El título VII de la misma Carta de las Naciones Unidas establece una autorización para el uso de la fuerza en respuesta a una amenaza para la paz o la seguridad internacionales.

¿Y de quién depende esa autorización? Pues, en teoría, debe ser el Consejo de Seguridad de la ONU quien autorice el uso de la fuerza, con el acuerdo unánime de los cinco países que son miembros permanentes del Consejo, es decir: Estados Unidos, Reino Unido, Francia, China y Rusia. Y digo en teoría porque, dado que todos los miembros permanentes tienen derecho de veto sobre las decisiones, en la práctica, rara vez se alcanza un acuerdo para una coalición internacional avalada por las Naciones Unidas. Esto ha dado lugar a frecuentes misiones bélicas que no cuentan con el beneplácito de la ONU (recordemos la guerra de Irak), y que no por ser ilegales se han visto frenadas.

Además, en ausencia de una actuación del Consejo de Seguridad, los tratados internacionales sobre la guerra establecen que los Estados pueden hacer uso de la fuerza únicamente en caso de defensa propia. Concretamente, el derecho a la defensa «en caso de un ataque armado» viene recogido en el artículo 51 de la Carta de las Naciones Unidas.

Por otro lado, tal como recuerda, en un artículo para el diario *La Vanguardia*, Timothy Edgar, del Watson Institute for International Studies, y que ha trabajado como asesor sobre ciberconflictos para la Casa Blanca, la defensa puede ser individual o colectiva. De este modo, alianzas defensivas como la OTAN están reconocidas por el derecho internacional. Concretamente, el artículo V de la Alianza Atlántica, firmada en 1949, contiene uno de los pasajes más importantes que se han escrito sobre política internacional al establecer: «Las partes acuerdan que un ataque armado contra uno o más de ellos en Europa o América del Norte, será considerado como un ataque contra todos ellos». Estas palabras dan fuerza de ley por primera vez a la «defensa colectiva» en la que se basará la alianza militar más poderosa y exitosa de la historia: la OTAN.

Este «todos para uno y uno para todos» permitió a los miembros de la alianza compartir riesgos y permanecer unidos a lo largo de varias décadas de vaivenes históricos y militares. Juntos han afrontado la guerra fría o la caída del muro de Berlín, y han dado una respuesta colectiva a los atentados del 11 de septiembre de 2001 en Nueva York y Washington.

Sin embargo, los ciberataques de Rusia contra Estonia en 2007 plantearon un nuevo desafío para la OTAN, uno para el que, por primera vez, no estaban preparados. De repente, uno de sus miembros era víctima de un tipo de ataque con el que no estaban acostumbrados a lidiar, y para el que no se había establecido un protocolo claro de actuación. Estonia es uno de los países más conectados de Europa y la mayoría de los ciudadanos gestionan todas sus actividades a través de internet, desde sus operaciones bancarias hasta su voto electoral. Y, de repente, todos los bancos estonios, todas las webs de los medios de comunicación y los sitios digitales del Gobierno habían sido víctimas de un ataque de denegación del servicio a gran escala.

Tras identificar a Rusia como responsable de los ataques, Estonia pidió ayuda a sus colegas de la OTAN. Al fin y al cabo, uno de los miembros del Tratado Atlántico estaba siendo atacado, y eso debe ser considerado como un ataque a la Alianza en su conjunto. Sin embargo, el resto de las partes de la OTAN consideraron que, en este caso, el capítulo V del tratado no podía ser aplicado porque nadie había muerto o resultado herido, y ninguna propiedad había resultado destruida o dañada. Se hizo más cierta que nunca esa sentencia de Cicerón: «*inter arma, silent leges*» («entre las armas, callan las leyes»).

## Si un ataque no está definido, no hay respuesta

La OTAN decidió que no merecía la pena arriesgarse a una guerra abierta con Rusia por un asunto que, aunque perturbador, pudo resolverse por completo sin perjuicio para nadie. En lugar de responder con la fuerza, la Alianza Atlántica decidió enviar a Estonia a un grupo de expertos informáticos para ayudar al país a restablecer sus redes, y emitió un comunicado en el que condenaba los ciberataques. Algún tiempo después, el Departamento de Diplomacia Pública de la OTAN creó una pequeña película sobre este episodio que llevaba el título de *Guerra en el ciberespacio*. No deja de ser irónico que la OTAN negara que los ciberataques de Estonia fueran un acto de guerra, pero después bautizara con ese sustantivo la película. Si se hubiera analizado de otra forma, con la ley en la mano, la OTAN tendría que haber respondido con la fuerza al ataque ruso.

Pero, entonces, ¿cuándo debemos considerar que un ataque constituye un uso de la fuerza merecedor de respuesta? Según el Tribunal Internacional de Justicia, en su dictamen (u opinión consultiva) sobre la legalidad o el uso de armas nucleares, emitido en 1996, las armas empleadas no son especialmente importantes, y un país no está obligado a emplear armas convencionales para lanzar un ataque armado.

De acuerdo con esta interpretación, los ciberataques de Rusia contra Estonia podrían encajar en la definición de «uso de la fuerza». Al fin y al cabo, como recuerda Timothy Edgar: «Los ataques a Estonia apuntaron contra servicios en línea esenciales del país, incluido el sector bancario. Fueron actos de sabotaje intencionados, dirigidos contra los sistemas de información de un país soberano en su propio territorio, al parecer, con el propósito de intimidarle y disuadirle de adoptar sus propias decisiones políticas».

Sin embargo, considerar un ciberataque como uso de la fuerza en el sentido tradicional, en el que disponen las leyes de la guerra, es un poco más complicado. Como señala Edgar, el derecho internacional está diseñado para limitar los conflictos, no para promoverlos. Por muy ilegales que fueran los ciberataques lanzados

por Rusia contra Estonia, calificarlos de conflictos armados podría traer consecuencias y sentar un precedente muy peligroso.

Por ejemplo, en junio de 2014, el banco J. P. Morgan Chase, uno de los más importantes del mundo y una pieza esencial del sistema financiero mundial, fue víctima de un ataque que comprometió la confidencialidad de unos 76 millones de cuentas corrientes y de siete millones de empresas. El Gobierno de Estados Unidos llegó a la conclusión de que el culpable más probable detrás de estos ataques era el Gobierno de Moscú. J. P. Morgan garantizó a los clientes que sus cuentas estaban protegidas, y aseguró que los hackers sólo habían podido hacerse con nombres, direcciones, números de teléfono y correos electrónicos, pero no habían podido acceder a las contraseñas ni a otra información sensible sobre las cuentas. Tampoco se habían llevado dinero.

Sin embargo, los piratas informáticos sí habían logrado acceder a más de noventa servidores internos, y también obtuvieron privilegios de administrador en un cierto número de sistemas del banco. Además, antes de que fueran descubiertos, los hackers se llevaron una lista de los programas y sus aplicaciones, que presumiblemente podrían utilizar para volver a entrar en los sistemas del banco. Al parecer, los intrusos podrían examinar los programas robados para buscar vulnerabilidades en ellos (los famosos *zero days*).

Vamos, se reconoció lo de siempre. Los hackers habían sido tan listos y tan avanzados técnicamente como para entrar en una de las empresas más seguras del mundo, pero luego no hicieron nada dentro, y sólo recopilaron información irrelevante que no te afecta si eres cliente del banco. Ya, claro. Moraleja: si eres cliente de este banco, yo que tú me preocuparía (y mucho).

En resumidas cuentas, no se trataba de piratas normales y corrientes, sino de lo que en el ámbito de la seguridad informática se denomina una «amenaza persistente avanzada», o APT (*advanced persistent threat*), por sus siglas en inglés. Como decimos, Washington identificó a Rusia como el origen de los ataques contra J. P. Morgan; sin embargo, nunca se han encontrado respuestas para la motivación de estos ataques. Puede que se tratara de un intento de robo, de un caso de espionaje económico o

de una represalia de Putin por alguna ofensa realizada por Estados Unidos.

No obstante, hay otra teoría más inquietante que explica estos ciberataques. Se baraja que pudiera tratarse de incursiones preliminares de un posible conflicto cibernético, lo que el Departamento de Defensa de Estados Unidos califica de «preparación del campo de batalla».

No cabe duda de que los ataques digitales contra J. P. Morgan se realizaron sobre una infraestructura civil y no militar o institucional. Sin embargo, los ataques podrían interpretarse como una amenaza de Putin a Washington. De acuerdo con esta lectura de los hechos, ¿podría considerarse el ataque de Rusia contra la entidad financiera como un uso de la fuerza merecedora de una respuesta militar?

## Amenazas y ataques preventivos

Es probable que los hechos sucedidos con J. P. Morgan te parezcan insuficientes para desatar una respuesta armada de Estados Unidos. Y tendrás toda la razón si así te lo parece. Sin embargo, en otras ocasiones, la frontera entre lo que puede ser considerado un acto de guerra y lo que no resulta mucho más tenue.

El Manual de Tallin dictaminó que los ataques llevados a cabo por el gusano Stuxnet contra el programa nuclear de Irán sí constituyen «uso de la fuerza». Esto significa que este tipo de ciberataques debe ser considerado ilegal, a no ser que Estados Unidos e Israel puedan justificar el ataque como una acción llevada a cabo en defensa propia ante la amenaza de que Irán pudiera estar planeando un ataque armado contra ellos. No sería descabellado, y, de hecho, Israel lleva años lidiando y protegiéndose de la amenaza de un ataque nuclear de sus vecinos árabes y persas.

Sin embargo, como expone Edgar, generalmente se sigue un criterio internacional según el cual un país sólo puede lanzar un ataque preventivo contra otro, sin esperar a que otro ataque en primer lugar, cuando el ataque se realiza «en defensa propia contra un ataque inminente». Y, en el caso del ataque de Israel y Estados Unidos contra las centrales nucleares iraníes, resulta difícil argumentar que existía una amenaza previa e inminente de Teherán.

Washington suele escudarse en que las consecuencias de demorar un ataque hasta que la amenaza sea inminente podrían ser catastróficas, una interpretación que es rechazada por la mayor parte de los países. Si desechamos, por tanto, los argumentos justificativos de Estados Unidos e Israel, tendríamos que concluir que el ataque llevado a cabo por el virus Stuxnet fue ilegal. Esto abre la puerta a otros dilemas. Si Stuxnet constituyó un uso de la fuerza contra un país soberano, ¿debemos considerar el gusano como un ataque armado que podría ser respondido militarmente por Irán empleando también la fuerza? ¿Qué diría la ONU de ello?

Los expertos del Manual de Tallin también se muestran prudentes sobre la adecuación de una respuesta militar a los ciberataques contra Irán. Al fin y al cabo, sostienen, el gusano no produjo

víctimas mortales, y los efectos sobre la población iraní fueron imperceptibles. En todos los casos, las recomendaciones de los expertos en seguridad abogan por adoptar las medidas que más contribuyan a reducir la inestabilidad. Seguramente, una respuesta armada por parte de Irán no resolvería el conflicto, no repararía el daño infligido y tampoco serviría de disuasión para futuros ataques. Por contra, un intercambio de ataques armados aumentaría peligrosamente el riesgo de una guerra abierta entre las dos partes implicadas.

## Incertidumbre y estrategia digitales

Lo que es evidente es que la aplicación de los tratados de guerra clásicos al nuevo contexto de la ciberguerra resulta insuficiente, resuelve pocas dudas y abre nuevos interrogantes. Es muy complicado discernir qué es susceptible de ser considerado una amenaza, a qué podemos llamar ataque armado o definir una situación de riesgo militar inminente. Del mismo modo, no tenemos argumentos suficientes para dictaminar qué ataques constituyen un reto para la seguridad nacional o cuáles comprometen la soberanía de los Estados. Por último, en un mundo crecientemente interconectado y globalizado, resulta especialmente arduo distinguir los ataques que tienen como objetivo infraestructuras civiles y los ataques dirigidos contra instituciones militares o gubernamentales de un país.

Según la Convención de Ginebra, las instalaciones de defensa o infraestructuras sobre las que se apoya una fuerza militar opuesta pueden ser objetivos válidos en una guerra, siempre que el ataque sea proporcionado. Sin embargo, ataques de envergadura contra infraestructuras civiles no pueden ser admitidos nunca.

Por otro lado, tampoco hay mucha certidumbre sobre cómo podríamos encajar el derecho internacional humanitario en la nueva guerra en el ciberespacio. Tal como nos recuerda Edgar, el derecho internacional establece «el uso de uniformes y el despliegue de banderas para permitir distinguir entre combatientes y civiles». ¿Cómo rayos se aplica esto a internet? ¿Deberían haber enviado los estadounidenses y los israelíes al gusano Stuxnet vestido de marine? Bueno, hubiera sido divertidamente absurdo, pero difícil de ejecutar. ¿Deben los Estados identificar en el código de los virus empleados en los ciberataques distintivos que permitan identificar su procedencia? Seguramente, sí, pero ¿cómo garantizar su cumplimiento? ¿Cómo protegemos las infraestructuras civiles de los ataques motivados por un contexto de ciberguerra?

La cuestión deja más preguntas que respuestas. Como ha señalado Dimitry Adamsky, profesor del Interdisciplinary Center de Herzeliya, en Israel, «asistimos a una revolución emergente en

asuntos militares, una innovación militar radical en la que las nuevas estructuras organizativas, junto con nuevos conceptos de operaciones, generalmente impulsados por nuevos tipos de armas, modifican de modo esencial la conducción de la guerra».

Por ello, a pesar de las limitaciones para circunscribir la ciberguerra en el marco teórico y legal de la guerra tradicional, en los últimos años la comunidad internacional ha hecho un esfuerzo por tratar de definir estrategias de actuación en caso de ciberconflictos.

En un artículo sobre ciberguerra, Stefano Mele, experto en ciberseguridad de la OTAN y del Gobierno italiano, afirmaba que, en la actualidad, «38 de los 196 Estados generalmente reconocidos a nivel mundial como soberanos han formalizado y publicado un documento estratégico en materia de ciberseguridad (las llamadas "estrategias cibernéticas")».

Mele explicaba que estas estrategias pueden analizarse a partir de los siguientes 13 pilares fundamentales:

- Identificar y clasificar las infraestructuras críticas que deben protegerse.
- Establecer tratados, leyes y normas de conducta nacionales e internacionales específicas para el sector de la ciberseguridad.
- Desarrollar las relaciones diplomáticas y reforzar las sociedades internacionales.
- Hacer hincapié en la protección de los derechos fundamentales, la intimidación o la libertad de expresión.
- Hacer hincapié en el ciberdelito.
- Tratar el ciberespacio como un dominio de guerra.
- Crear estructuras políticas y de decisión para hacer frente a las amenazas.
- Desarrollar la disuasión para prevenir conflictos en el ciberespacio.
- Subir los niveles de seguridad, fiabilidad y resiliencia de las redes y de los sistemas informáticos.
- Reforzar la posibilidad de compartir la información (en especial entre las entidades públicas y privadas), las alertas tempranas

y la capacidad de reacción en casos de ataque.

- Aumentar la conciencia pública de la amenaza y la importancia de la ciberseguridad.
- Crear o incrementar el número de las figuras profesionales del sector de la ciberseguridad.
- Fomentar la innovación, la investigación y el desarrollo nacional en el sector de la ciberseguridad.

Además, entre los 28 Estados miembros de la Unión Europea, 18 de ellos tienen una estrategia digital formal, es decir, más de la mitad del total, y casi la mitad respecto a los 38 países de la comunidad internacional que cuentan con estrategias de este tipo. Parte de la explicación a estos datos viene de la «Estrategia de ciberseguridad de la Unión Europea», que recomienda a los Estados miembros desarrollar estrategias nacionales en materia de seguridad en el ciberespacio.

## La ciberdefensa de la OTAN

Buena parte del potencial militar para la ciberdefensa de la OTAN está basado en la creación del Centro de Excelencia de Ciberdefensa, que fue puesto en marcha en Tallin a raíz de la serie de ataques cibernéticos dirigidos por Rusia contra Estonia.

La Alianza Atlántica lleva ensayando ejercicios de defensa cibernética desde entonces. En 2010, la OTAN realizó su tercer ejercicio, que llevó por nombre Cibercoalición 2010 (*The Cyber Coalition of 2010*). En los ensayos, la organización atlántica simuló ciberataques contra la Alianza para poder poner a prueba y testar su capacidad de respuesta ante episodios de guerra digital.

Posteriormente han tenido lugar nuevas maniobras de estas características, como las llevadas a cabo por la Cibercoalición 2013. Los ejercicios duraron tres días y fueron dirigidos desde el Centro de Excelencia de Ciberdefensa, en Estonia. Los ensayos son muy relevantes para la OTAN, y prueba de ello es que en ellos participó personal de más de treinta Estados y unos cuatrocientos expertos en asuntos legales y gubernamentales, además de, por supuesto, los especialistas informáticos de toda la Alianza.

Por medio de un comunicado, la OTAN declaró entonces que: «Con unos cien participantes en Tartu [Estonia] y más de 300 en las capitales nacionales de 32 países, la Cibercoalición 2013 es el mayor ejercicio de este tipo respecto al número de países participantes».

Este tipo de ejercicios se centra especialmente en comprobar el nivel técnico de la OTAN y sus socios, así como en verificar cómo los participantes coordinan sus esfuerzos ante este tipo de amenazas. Como si se tratara de un escenario de un juego de guerra, durante las maniobras se llevan a cabo «múltiples intentos simultáneos de infiltración en las redes de información a través de diferentes técnicas de guerra cibernética, incluyendo las redes de bots [robots] y sitios web infectados con *malware*», según explicó Roland Murof, un portavoz militar de las Fuerzas de Defensa de Estonia. Y para que nadie se diera por aludido o se sintiera ofendido, Murof también aclaró que las simulaciones tienen lugar en escenarios ficticios, por

lo que «los atacantes son organizaciones inventadas apoyadas por naciones ficticias y no tienen ningún vínculo con el mundo real».

Desde que tuvieran lugar los ciberataques contra Estonia, la OTAN ha puesto en marcha sistemas de respuesta rápida, al mismo tiempo que ha trabajado en una estrategia política a largo plazo, que fue acordada durante la cumbre de Lisboa de 2010. Sin embargo, el esfuerzo se ha realizado sobre todo en materia de seguridad y defensa, mientras que se ha descuidado sensiblemente la estrategia ofensiva; o bien ésta se mantiene tan en secreto que ni siquiera se comparte en el seno de la OTAN.

Hasta hace poco, la OTAN todavía no había decidido si un ataque cibernético contra un miembro de la Alianza debía implicar una respuesta colectiva, tal como se indica en el artículo V del Tratado de Washington. La seguridad cibernética se trataba como un tema de responsabilidad nacional, pese a la interconexión de las redes entre los Estados miembros.

Sin embargo, recientemente, la Alianza Atlántica ha dado un paso adelante en este sentido, declarando que los ataques cibernéticos serán abordados con idéntico trato al que reciben los ataques dirigidos con armamento convencional, relacionando la cuestión con el título V del Tratado Atlántico, y abriendo la puerta a futuros enfrentamientos militares por casos de ataques en la red. Tras esta última declaración cabe esperar que, de producirse un nuevo incidente como el que tuvo lugar entre Rusia y Estonia, la OTAN procedería a una respuesta militar, amparada en el principio de «todos para uno y uno para todos».

Pero también esto quiere decir que si eres un veinteañero travieso, sentado frente a tu ordenador con unas patatas Pringles y jugando a vulnerar la seguridad de sitios críticos, corres el riesgo de que se considere que estás cometiendo un acto de guerra y, por lo tanto, protocolo en mano, puedan meterte un misilazo. Y eso sería un enorme desperdicio de Pringles. O sea, que tú mismo.

6

# ¡Gracias, tecnología, por convertirnos en un saco de boxeo!

A estas alturas de la lectura es posible que compartas conmigo la idea de que el vertiginoso avance tecnológico nos sitúa en un escenario hostil en el que somos, incluso sin pretenderlo, el eslabón débil de una cadena global de la que, posiblemente, ni siquiera querríamos formar parte.

Llegados a este punto, la pregunta es evidente: ¿qué podemos hacer para protegernos y estar a salvo en el ámbito de internet y las comunicaciones? Y debo reconocer que la respuesta es poco alentadora: NADA.

Déjame matizarlo con detalle. No podemos hacer nada que garantice nuestra privacidad, nuestra seguridad o la inviolabilidad de nuestros datos. Todo es vulnerable y todo es accesible. Incluso aunque no estemos conectados a internet. Lo que sí que podemos hacer es ponérselo un poquito más difícil a quienes quieran vulnerar nuestra privacidad, es decir, según lo denomino yo, podemos «entrenarnos en artes marciales», que no es otra cosa que aprender y ensayar determinadas técnicas de «defensa» en internet. Por supuesto, tal entrenamiento no es garantía absoluta de nada, e incluso puede crearnos una falsa sensación de seguridad. Pero, por decirlo así, la cosa es que, si tienes que recibir una paliza, que al menos tenga que dártela alguien más parecido a Bruce Lee que a Pocoyó. Vamos, que se trata de dejar el pabellón lo más alto posible

y ponerlo un poco difícil, de que cualquier «matao» no te pueda meter mano.

Eso sí, por mucho que «entrenes» y seas capaz de ponerlo difícil, debes saber que, si tu información es especialmente valiosa o si en un momento dado desarrollas una actividad que puede ser de interés para servicios de inteligencia, grandes corporaciones o cibercriminales con medios, las posibilidades de que tu información se vea comprometida son muy altas, y que se trata sólo de una cuestión de tiempo, hagas lo que hagas.

Históricamente se ha dicho que la información es libre y que, como tal, debe fluir libremente. Es así, pero lo que no se dice es que la información tiene unas claras limitaciones de «movimiento»; la información puede transmitirse de manera manual mediante la intervención física del ser humano (lápices de memoria, discos duros, libros, etc.), por ondas (satélites, antenas, etc.) o por cables eléctricos, telefónicos o de fibra óptica (que, en cierto sentido, incluyen las redes wifi, ya que sus puntos de acceso o enrutadores reciben los datos generalmente por cable). En definitiva, la interconexión mundial no deja de ser más que un entramado de decenas de miles de redes conectadas por cables, antenas y satélites más o menos sofisticados.

Hace años se decía que todo lo que está conectado a la red es «hackeable». Y es cierto. Por eso, cada vez que había algún incidente de *hacking*, muchas personas se preguntaban por qué determinados equipos estaban conectados a la red. La respuesta es obvia: es necesario que lo estén para su correcto funcionamiento.

Aunque, para estar protegidos, lo primero que tenemos que hacer es defendernos de nosotros mismos, de nuestros errores a la hora de usar las redes. Eso comienza por elegir claves seguras para nuestros accesos, correos, archivos… La clave más utilizada es «12345», y la segunda más usada es «password». Eso, evidentemente, hace que sea absurdamente fácil el poder acceder a todos nuestros archivos, nuestra información e incluso nuestros datos bancarios.

Lo ideal es que utilicemos una frase sin sentido y que seamos capaces de recordar, modificando algunas letras por números y, si es

posible, con la utilización de mayúsculas y minúsculas e incluso símbolos. Y, por el amor de Dios, aunque no quieras complicar tanto tu contraseña, no uses el nombre de tus hijos, el año que nacieron, etc. ¡Es carne de cañón!

Al margen de que compliquemos lo máximo la clave para acceder a nuestros datos en diferentes servicios, resulta fundamental no utilizar la misma clave para varios servicios. Según un reciente estudio elaborado en el MIT (Massachusetts Institute of Technology), el 92 por ciento de los usuarios reconoció que utilizaba la misma clave para todos sus servicios. Una vez que un proveedor ha sido comprometido, quedas totalmente en evidencia, y completamente desprotegido.

Si tenías cuenta en Geocities, MySpace o Second Life, por poner algunos ejemplos, debes saber que esa cuenta, con tu contraseña y dirección de correo electrónico vinculado a ella, circula libremente por internet y habrá sido vendida decenas de veces. Sólo hace falta una brecha de seguridad, una única vez, para que todos esos datos circulen; y si los usas, por ejemplo, asociados a tu tarjeta de crédito en servicios de compra online, estás en riesgo.

Reconozco que tenía cierta soberbia personal en cuanto a la seguridad hasta hace un par de años. Sí, yo era de los que pensaban que esto no iba conmigo y que tenía suficiente cuidado de no correr riesgo alguno. Una mañana de septiembre de 2014 recibí una llamada de uno de mis técnicos. Se habían filtrado unos cinco millones de contraseñas de Gmail.

—Ah, muy bien. Pasa casi todos los días —respondí sin prestar mucha atención.

—Sí, Alejandro, pero hay una herramienta online para ver qué correos han sido vulnerados, y el tuyo es uno de ellos. Entra inmediatamente.

Y así era. Accedí a la herramienta y efectivamente, allí estaba mi correo electrónico y mi contraseña. Atónito la cambié. Ése, por cierto, fue el día que también aprendí que no debía usar la misma en varios servicios, cosa que sabía perfectamente, pero a la que no

hacía ni caso. Conclusión: no recuerdo cuánto tiempo me pasé cambiando contraseñas…

No pasó nada más, que yo sepa; pero la cara de idiota que se te queda es digna de análisis. Me pasé semanas intentando averiguar si había hecho yo alguna tontería (como instalar alguna aplicación no segura) o si se trataría de un fallo de seguridad de Google. Al parecer, estos datos se fueron recopilando desde varias fuentes durante años, y se pusieron en valor contra Gmail. Es decir, se trató de fallos de seguridad en otros servicios, en búsqueda de correos electrónicos «@gmail.com» para comprobar si esos usuarios estaban utilizando la misma contraseña en el servicio comprometido y en Gmail.

La explicación ya es lo de menos. Fue un interesante baño de humildad. Desde ese momento tomo más precauciones que antes. ¡Vaya si lo hago!

Así que estamos todos expuestos y todos conectados. Lo que sí ha cambiado hoy en día es que no es tan importante si las cosas están conectadas a la red o no, sino que lo relevante es si están seguras. Para ello, una de las cosas más seguras que podemos hacer es encriptarlas. Lo primordial ya no es dónde escondemos lo que no queremos que sea encontrado, sino, más bien, partiendo de la base de que será encontrado, dónde escondemos la llave de esos archivos, aunque estos estén en una ubicación conocida. El acceso es la clave, y por lo tanto la clave es saber guardar las llaves.

Esto no es nuevo. Hace ya treinta años, al enviar una carta corríamos el riesgo de que el cartero la abriera. Ahora damos por hecho que lo hará; y lo que pretendemos es que, cuando la abra, descubra una serie de caracteres indescifrables e inútiles para él. Nuestra información viaja frente a las narices de cientos de miles de potenciales carteros. Si está expuesta, que no tengan la llave para abrirla.

La Wikipedia define la criptografía como «la ciencia que se ocupa de las técnicas de cifrado o codificación destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados. Estas técnicas se utilizan tanto en el arte como en la ciencia. Por tanto, el único

objetivo de la criptografía era conseguir la confidencialidad de los mensajes». Hoy en día, a eso es a lo máximo que podemos aspirar si se están dedicando recursos suficientes a localizar nuestra información; partiendo de la base de que acabarán accediendo más pronto que tarde a ella, centrémonos en que no pueda ser descifrada.

Es por ello que, en comunicaciones que pretenden ser seguras, resulta fundamental su encriptamiento. Eso no quiere decir que sean ciento por ciento seguras. El programa PGP ofrece varias opciones de tamaño de cifrado. A mayor tamaño de cifrado mayor seguridad, por defecto podemos elegir codificaciones desde 384 a 4.096 bits.

Las llaves de PGP más básicas, como las de 384, 512 y 728 bits, no son tan seguras; y se ha demostrado que ya son vulneradas con ordenadores personales de última generación. Por ello, lo ideal es trabajar con llaves de al menos 2.048 bits, que posiblemente aguantarían el tipo contra los ordenadores más avanzados del mundo durante varios años, impidiendo descifrar la información. Dado el esfuerzo que llevaría, y teniendo en cuenta que las llaves de PGP caducan cada cinco años, ésta es una opción más que razonable. Pero ojo, eso es así a día de hoy, y se espera que lo siga siendo durante los próximos años, aunque ya hay proyectos de computación cuántica que esperan poder multiplicar exponencialmente la capacidad de procesos de los ordenadores, y eso lo cambiaría todo.

El uso de PGP en las comunicaciones, pese a remontarnos a casi los orígenes de internet tal y como lo conocemos (PGP originalmente fue diseñado y desarrollado por Phil Zimmermann en 1991), no está realmente extendido. Se considera que sólo el 2 por ciento de los internautas lo utilizan en sus comunicaciones. Usarlo tiene una parte negativa, y es que llama la atención. Las personas que se comunican de manera cifrada captan rápidamente la atención de los gobiernos y las fuerzas policiales. Se dice que existen listas de usuarios habituales de PGP en las que se está presente simplemente por utilizar criptografía. Y es algo lamentable que se deduzca que algo turbio tratas de ocultar sólo por el hecho de buscar una mayor privacidad.

Si no usas PGP o no estás mínimamente familiarizado con este tema, es posible que estés dejando pasar alguna buena oportunidad. Eso lo sabe bien Glenn Greenwald, periodista de *The Guardian* que estuvo a punto de perder la exclusiva de su vida, con la que luego ganaría el Premio Pulitzer por Servicio Público en 2014, al ser contactado por Edward Snowden pero no querer instalarse PGP para comunicarse. Le pareció complicado y no tenía tiempo para atender a un «pirao» que le mandaba correos electrónicos y pedía una comunicación segura. Snowden llegó a enviarle tutoriales e incluso un vídeo «para *dummies*» (o «para tontos») con el que poder entender cómo instalarlo. Pasaron muchos meses antes de que Greenwald retomara el interés por el asunto, gracias a la ayuda de Laura Poitras, que sí sabía utilizar la encriptación de correos electrónicos. El resto es ya historia.

No sólo tenemos que protegernos de criminales, de empresas interesadas en nuestra información —por ejemplo nuestra competencia—, agencias de publicidad agresiva e incluso agencias de inteligencia, también hay un gran riesgo en nuestros proveedores de servicios. Si usas correo electrónico y tienes un proveedor de telefonía móvil, otro de cable…, entonces tienes decenas de posibilidades de que los empleados de estas compañías puedan acceder a tus posiciones. Bien por algún interés, bien sólo por diversión.

En 2010, Google decidió despedir a David Barksdale, un ingeniero de veintisiete años de edad, por acceder a posiciones, manipular y acosar a cuatro menores de edad que había conocido en la red. Si bien no era la primera vez que sucedía en la compañía de Mountain View, sí fue la primera vez que hubo menores implicados. El acosador aprovechó sus privilegios en Google para hacerse con sus listas de contactos, chats, correos y conversaciones, llegando a suplantar a algunos de dichos contactos.

Según declaró el vicepresidente de ingeniería de Google Bill Coughran, «hemos despedido a David Barksdale por quebrantar las estrictas políticas internas de privacidad de Google. Controlamos cuidadosamente el número de empleados que tienen acceso a

nuestros sistemas, y actualizamos con regularidad nuestros controles de seguridad. Dicho esto, siempre será necesario que un número limitado de gente tenga acceso a estos sistemas si queremos que funcionen correctamente, por eso tomamos tan en serio cualquier violación». Como conclusión: que estas cosas pasan, y con mucha más frecuencia de lo que crees, aunque no trasciendan. Vamos, que no lo dudes: si tienes una expareja que trabaja en un proveedor de servicios de internet (ISP), una compañía de telefonía móvil, un banco…, ¡por supuesto que casi seguro que ha accedido a tus posiciones! Aunque sea sólo por cotillear.

Y aunque de forma absurda puedas confiar al ciento por ciento en todos los empleados de tus proveedores de servicios, que sepas que debes confiar también en los de las personas a las que escribes y con las que tienes contacto, ya que el riesgo existe en el punto de origen y de destino. ¡Incluso en puntos intermedios! Otros ISP que hacen de enlace mediante puntos neutros, que son conmutadores que sirven para el intercambio de archivos entre proveedores de servicios, podrían cometer la misma deslealtad con tu información.

## Un sistema de localización que, además, sirve para hablar por teléfono

Aunque sería ridículamente temerario compararlo con la rueda o el fuego, no encuentro muchos inventos en los últimos cien años que nos estén cambiando la vida tanto como la telefonía móvil y la irrupción de los teléfonos inteligentes, o *smartphones*.

En la Unión Europea, España es líder absoluto en penetración de *smartphones*, con un 81 por ciento de teléfonos inteligentes sobre el total de móviles, lo que supone diez puntos por encima de la media, según detalla el informe «La sociedad de la información en España», de la Fundación Telefónica.

Todo lo que es bueno es ilegal o engorda, y en el caso de los *smartphones* no podría ser de otra forma. En cierta ocasión, un agente del CNI me comentó, con una pícara sonrisa en la boca mientras observaba mi iPhone: «No sabía que tú también llevabas un aparato de monitorización y geolocalización. Creo que, además, incluso puedes hablar con él por teléfono». La conversación llamó mi atención y se fue alargando. Tenía lógica; si no quieres que se sepa que has estado en un sitio, empieza por no llevar tu teléfono y dejarlo en casa. Tras sus detalladas explicaciones y ejemplos del uso, en su día a día, de estos terminales de terceros, comprendí por qué él llevaba un teléfono móvil de otra generación en el bolsillo. Tanto me interesé por el tema y por esa diferente manera de volver atrás en el tiempo, que acabé comprando un Nokia 3100 de segunda mano en la red. Con él no sólo estoy (algo) más protegido en determinados momentos y respecto a determinado tipo de comunicaciones, sino que, además, cuando estoy aburrido puedo perder el tiempo jugando al mítico Serpiente. Lo veo como algo *vintage*, algo así como un regreso a 2003. Por supuesto conservo mi iPhone, pero hay ocasiones que son perfectas para dejarlo en casa y utilizar mi reliquia móvil. De hecho, el citado agente quiso complementar mi adquisición con un curioso regalo: una tarjeta SIM. Sólo me dijo: «Úsala con tranquilidad. La he comprado a un proveedor de confianza en La Latina. Está a nombre de una chica

rumana; si no haces tonterías que lo evidencien, nadie sabrá que esta línea es tuya». Poco más puedo añadir, está todo inventado.

Debes tener en cuenta que la mayoría de los teléfonos móviles actuales revelan tu ubicación precisa incluso estando fuera de cobertura o desconectados. Son los auténticos «pepitos grillo» del siglo XXI. No hay nada mejor para poderlo saber todo de una persona que acceder a su teléfono móvil de manera física o de manera virtual, con *software* diseñado a tal efecto. Algunos teléfonos incluso vienen viciados ya de fábrica; por una cantidad relativamente asequible, en tiendas de seguridad venden terminales espía, con modificaciones de *hardware* y *software* que permiten grabar y monitorizar toda la actividad de los mismos, lo que incluye: grabar en un mapa dónde está la persona en cada momento; acceso a la cámara y las fotos; tomar de forma remota imágenes en determinados momentos sin que la víctima lo sepa; recibir archivos con las llamadas de teléfono; recibir por correo electrónico los mensajes (SMS o de Whatsapp) enviados o recibidos, etc. Y todo ello gestionando el terminal mediante un panel remoto, y con «garantía de "indetectabilidad"». Hay servicios similares basados en aplicaciones que se deben instalar en el terminal de la víctima, no en el teléfono. De manera que el simple hecho de poder acceder al terminal unos minutos ya hace que pueda instalarse el *software* que habilita un seguimiento total. Ningún tipo de terminal está a salvo, esto sucede con iPhone, Android y BlackBerry. En la red aparecen periódicamente noticias e informaciones que, por interés comercial, intentan explicar que unos terminales son más seguros que otros. La realidad es que ninguno está a salvo.

Puede parecer una película de ciencia ficción o de espías, pero estos terminales intervenidos están a la orden del día. Sólo hay que ver la cantidad de juicios por divorcio con infidelidades de por medio en los que son mencionados.

Otro de los usos más frecuentes es el control de empleados. La ley obliga a que el empleado tenga conocimiento de si el terminal que se le ha facilitado monitoriza toda su actividad. Ni que decir

tiene que la ética y la ley no van de la mano. Generalmente, si alguien quiere espiar a otra persona no suele ponerle en preaviso.

Este tipo de terminales tienen también un uso denominado «caja negra», que consiste en grabar toda la actividad del mismo para, en caso necesario (un accidente, un secuestro, etc.), poder acceder a ella incluso aunque el teléfono sea destruido. Se anuncian con toda impunidad en internet como «la opción perfecta para vigilar a su hijo, su cónyuge o sus empleados».

Pero, del mismo modo que hay todo tipo de teléfonos y aplicaciones espías, en el mercado podemos encontrar terminales que se comprometen con la seguridad de nuestras comunicaciones. Es el caso del Blackphone, un terminal diseñado por Silent Circle, creadores del PGP, que promete encriptar todas tus comunicaciones. Se trata de un teléfono que funciona sobre una versión modificada de Android llamada PrivatOS, que añade capas de seguridad que encriptan nuestros datos y las transmisiones que realizamos con él. Hoy en día, el uso de este tipo de soluciones de encriptación para telefonía móvil es mínimo.

Pese al uso de la criptografía, y pese a todas las medidas de seguridad que quieras establecer, no confíes en tu propio móvil, ¡ni en el de las personas de tu alrededor! En una reunión de trabajo muy confidencial, la única manera de tener certeza de que no sois más oyentes que los que estáis sentados a la mesa es dejar los teléfonos móviles en otra habitación, o, mejor aún, en un microondas con la puerta cerrada, ya que así la llamada jaula de Faraday impide fehacientemente que el móvil pueda estar en uso controlado de manera remota y grabando o transmitiendo. Otra alternativa es un frigorífico a –15 °C. Determinadas empresas que compiten por contratos cada vez más importantes tienen ya salas seguras, que son jaulas de Faraday en sí mismas, con fibra metálica en las paredes para impedir que nada de lo que allí sucede pueda trascender en ningún caso.

**Págate una conexión, no seas cutre…, ¡o sufre las consecuencias!**

El caso es que, elijamos el teléfono que elijamos, todos los carga el diablo. A no ser que nos hayan dado un terminal ya preparado de fábrica para espiarnos, con lo que poco habría que hacer, el eslabón más débil seguimos siendo nosotros. Aunque tengas tu móvil al día, uses antivirus, no descargues programas que puedan comprometer la privacidad, etc., debes tener especial cuidado con tu conexión, y sobre todo con conexiones a redes wifi gratuitas y/o compartidas. Por ejemplo, la wifi gratis de la cafetería, del aeropuerto…, pero también la red de tu oficina.

Sé que pasar horas muertas en el aeropuerto cuando el vuelo sale con retraso es muy pesado, pero sería muy mala idea conectarse a la wifi del mismo y, por ejemplo, hacer una compra desde tu tableta o tu móvil, y, por supuesto, desde los equipos públicos del aeropuerto.

Cualquier red compartida es por defecto insegura, y cualquier persona conectada a esa misma red puede usar técnicas de ataque denominadas «*man in the middle*» (o «intermediario») para, sin necesidad de tener conocimientos informáticos muy avanzados y con sólo el uso de un par de programas, acceder a tu terminal y tener la capacidad de poder interceptar tus comunicaciones y suplantarte en la red.

En su libro *El pequeño libro rojo del activista en la red*, Marta Peirano da algunos consejos cuando, como medida de emergencia, tenemos que conectarnos a una red wifi pública. Estos son algunos de ellos.

1. **No lo hagas.** Si viajas con frecuencia, hazte con un rúter o un pincho USB 3G propio.
2. **Usa protección.** No garantiza nada, pero es suicida conectarte a una red wifi pública sin cortafuegos y antivirus actualizado.
3. **Desactiva la tarjeta wireless.** No permitas que se conecte automáticamente.

4. **Evita redes abiertas.** Especialmente las que tienen nombres como «Pincha aquí», «Internet gratis» y cosas por el estilo. Si dudas, pregunta a un responsable cuál es la red del establecimiento.
5. **Si hay varias redes...** Elije la que tenga el protocolo de seguridad más robusto. De menos a más WEP, WPA y WPA2.
6. **Cuidado con lo que compartes.** Teóricamente, las carpetas compartidas de tu equipo no deberían ser un riesgo, pero…
7. **Ojo a las DNS.** Hay estafadores que te redirigen a otros sitios en este tipo de redes donde crees estar en entornos de empresas seguras y puedes llegar a introducir tus datos.
8. **Usa TOR.** Si lo haces, aunque intercepten tus datos, estos serán poco útiles. Nunca sabrán de quién son.

## Pero yo estoy protegido porque uso TOR y cifro mis discos duros

¡Bien! Si usas TOR y cifras tus discos duros… ¡eres un campeón! Lo único que sucede es que eso es lo que decían los usuarios de Skype antes de 2011. Y lo que nos enseña eso es precisamente que nada es seguro, y que lo que es seguro hoy puede no serlo mañana. Se considera que las comunicaciones encriptadas de Skype fueron inaccesibles para los servicios de inteligencia durante muchos años. Los papeles de Snowden demostraron después que, en cuanto Microsoft compró Skype, la barra libre para los servicios de inteligencia estadounidenses estaba servida.

TOR es una manera de minimizar los riesgos, y, aparentemente, hasta la fecha no se ha logrado romper su encriptación. Sí han tenido problemas con ello determinados usuarios, pero siempre se ha atribuido a mal uso de TOR.

Ejemplos del mal uso de TOR son: compatibilizarlo con el uso de Java o con plugins de ciertos programas (especialmente de Flash y Realtime), abrir adjuntos mientras estás en TOR, etc. Es decir, aunque estés en un entorno seguro, es posible que, sin saberlo, cometas una imprudencia que lo haga inseguro en un momento dado.

Sobre el cifrado de información del disco duro, las memorias USB, etc., es una buena solución si realmente trabajas con información muy sensible. Es más, diría que es la mejor solución. Si por algún motivo la información a la que tienes acceso es muy codiciada, como ya mencioné antes, lo que hay que hacer es dedicar recursos a encerrarla bajo llave, no a esconderla.

Para ello, una muy buena solución es usar un programa de encriptación denominado TrueType. Eso sí, una persona que encripta sus archivos siempre llama la atención. Si bien es cierto que nadie tiene que ver lo que tienes en tu ordenador, imagina que por algún motivo los servicios de seguridad te exigen acceder a tu equipo (cosa que hoy en día empieza a ser habitual en Estados Unidos). Si al encenderlo todo está encriptado, igual te pasas unos días allí mientras recibes todo tipo de presiones y amenazas para

desencriptarlo. Encriptar tus datos es algo poco habitual y muy llamativo.

Del mismo modo, hay que prestar especial atención a las cosas que se eliminan. Lo que borres de tu disco duro, casi siempre puede ser recuperado. De hecho la mejor manera de garantizar que algo ha sido borrado es sobrescribir otra cosa justamente encima. El hecho de que las informaciones eliminadas, incluso en discos formateados, puedan ser recuperadas se conoció después de un incidente que dejó en un ridículo «sideral» a los servicios secretos alemanes, cuando un estudiante de la ciudad alemana de Potsdam adquirió a través de la tienda de subastas en internet eBay un disco duro de 20 GB atestado de datos confidenciales de la policía de Brandeburgo. El comprador, un joven estudiante de informática, se dedicó a extraer los datos del disco duro antes de hacer su propio formateado y descubrió cientos de archivos confidenciales de la policía.

Las empresas de seguridad especializadas en borrado de datos sugieren que los dispositivos con contenidos personales deben formatearse al menos ocho veces. Yo, sin ánimo de llevarles la contraria, sugiero una solución más rápida y menos técnica: un golpe en seco al cabezal del disco duro es la manera más segura de que nadie podrá utilizarlo de nuevo. Si, tal vez es menos sutil, pero resulta más eficiente.

## Un dron con Antrax como regalo de cumpleaños

Imaginemos una escena a finales del año 2009. Un dron acaba una misión de éxito en Afganistán. El comandante en jefe del ejército estadounidense sonríe, la misión ha sido un éxito. Se han destruido los objetivos y se ha eliminado a un terrorista que estaba siendo perseguido. Todo ello gracias a la tecnología, sin arriesgar vidas de soldados sobre el terreno. Es cierto que ha habido algunas víctimas colaterales entre la población local al dar caza y eliminar al terrorista. Pero, bueno, eso parece un mal menor, e igual ni siquiera trasciende. «Seguro que, dentro de unos años, nuestros drones mejoran en seguridad», piensa el comandante en jefe.

Eso espero yo también, ya que un reciente estudio de la ONG británica pro derechos humanos Reprieve alerta de que, para asesinar a 41 terroristas de AlQaeda en Pakistán, Yemen, Libia y Somalia, los drones norteamericanos han matado o herido a 1.147 inocentes. Las citadas víctimas colaterales.

Aquel hombre, el comandante en jefe de nuestra historia, tiene nombre y apellidos, e igual te suenan, porque sale de vez en cuando en la televisión. Es un tal Barack Obama, quien, un año antes, había jurado el cargo como presidente de la nación más poderosa del mundo, y una de las pocas que contaba en aquel momento con un enorme arsenal de aviones no tripulados plenamente operativos.

En aquellos años, al escuchar el sonido de los drones sobre la Casa Blanca, Obama debía de mirar al cielo y sonreír con orgullo, recreándose en la supremacía militar de su ejército. Con la misma sonrisa que yo utilizo con cierta malicia al recordar que a ese mismo hombre, ese mismo año, vergonzantemente se la hacía entrega del Premio Nobel de la Paz.

Enero de 2015. No ha pasado siquiera una década, y Obama ha escuchado de nuevo el curioso sonido de un dron sobre la Casa Blanca. Esta vez no sonríe, de hecho es posible que esta vez ni siquiera se haya enorgullecido. Juraría que se debe haber asustado (yo lo haría). El servicio secreto ha corrido a ocultarle en el búnker

de la Casa Blanca en medio de una enorme crisis de seguridad. ¿Un atentado?

Tras las pertinentes averiguaciones llega una tensa calma. Ha sido una falsa alarma. No se trataba de un ataque terrorista contra el corazón de la política estadounidense. No había explosivos ni armas. Simplemente era un pequeño dron recreativo, que había entrado en el espacio protegido sin ser detectado por los servicios de seguridad y, con sus sólo 1,3 kilogramos de peso, se había estrellado contra la Casa Blanca. Un desgraciado accidente.

Si lugar a dudas, los más jóvenes de los servicios de seguridad resoplarían tranquilos. Pero es muy posible que los miembros de seguridad con más experiencia mantengan aun hoy un rictus muy tenso pensando en aquello. Ha quedado probado lo que era un secreto a voces. A fecha de hoy, proteger a altos cargos o infraestructuras críticas de un posible ataque terrorista por medio de drones es una labor imposible, física y tecnológicamente. Es sólo cuestión de tiempo que alguien pueda llevar a cabo estas acciones.

Tal es la creciente preocupación que grandes acontecimientos deportivos como la Super Bowl se juegan en recintos que son declarados como «zonas libres de drones» por las autoridades, que prohíben su uso recreativo en un amplio radio de seguridad alrededor del evento, lo cual incluye poder derribar estos aparatos en el caso de que violaran ese espacio aéreo. Y tal como se las gastan los norteamericanos, igual también derribarían a quien los manejara.

Lo que ha ocurrido es un efecto bumerán basado en la ley de Moore que rige la velocidad exponencial de los avances tecnológicos y la rapidez con la que estos se suceden. Hace poco más de una década, un drone RQ-4, como los usados en Irak y Afganistán, tenía un coste de más de cien millones de dólares. Hoy, por menos de diez mil dólares se pueden comprar aparatos que tienen algunas prestaciones similares (no todas, ¡no van a lanzar misiles, por ejemplo!).La tecnología se ha popularizado y está al alcance de todos. Y, como sabes, la tecnología nueva y disruptiva tiene esa dualidad de poder ser empleada para el bien y para el mal. Lo que era una ventaja militar evidente, hoy forma parte del arsenal de la

gran mayoría de los ejércitos del mundo, y también se ha extendido su uso civil, y eso incluye desde la utilización recreativa hasta la utilización para actividades ilícitas.

Y es que «los malos», como hemos comentado con antelación, siempre han sido *early adopters.* Por ese motivo encontramos drones en los sitios más recónditos y con los usos más creativos que se pueda imaginar.

Estos pequeños ordenadores voladores son utilizados por mafias organizadas para introducir drogas, armas o teléfonos móviles en cárceles de Brasil. Las vallas electrificadas que protegen el interior de estos recintos están pensadas para aislar a los presos del contacto exterior, pero, desde luego, eso era antes de la «era dron».

En muchos países del mundo, los cárteles de la droga ya no necesitan contratar mulas para cruzar la frontera. Así, se han detectado intentos de introducción de hachís en España por el estrecho de Gibraltar utilizando drones, y se sabe que los cárteles de la droga mexicana utilizan estas pequeñas naves no tripuladas para pasar cocaína a California desde Tijuana, muy cerca de la frontera. Sin embargo, no es que tengamos constancia de estos hechos por la capacidad de nuestras autoridades para detectarlos. Más bien todo lo contrario, ya que sólo han quedado probados cuando, por fallos técnicos, condiciones meteorológicas adversas o poca habilidad de los operadores, los drones se han precipitado al suelo dejando en evidencia su uso y cargamento. La época en que los narcos necesitaban arriesgar a sus hombres, sus helicópteros y sus lanchas rápidas para huir de la policía parece estar superada.

Por supuesto, el 90 por ciento del uso de los drones es legal (aunque, a veces, perverso; por ejemplo, hay ayuntamientos que los usan para sobrevolar las propiedades de sus vecinos en busca de piscinas no declaradas o ampliaciones de vivienda ilegales para así sancionarlos…,¡malditos!). Aun así, se abre la puerta al uso delictivo y, lo que es mucho más inquietante, al uso con fines terroristas de esta ventaja tecnológica. Es muy probable que dentro de una década tengamos la misma preocupación sobre los coches no tripulados que varias compañías, entre ellas Google, están probando hoy en todo el mundo. También estas máquinas pueden utilizarse de

manera remota y/o programada, y pueden escapar al control de las autoridades y ser usadas con fines delictivos o terroristas.

No sólo Obama ha tenido que preocuparse por los drones. Y eso que la Casa Blanca ya está ensayando (aunque parece que con poco éxito) la posibilidad de utilizar un pequeño escuadrón de drones para proteger su espacio aéreo.

En septiembre de 2013, cuando los miembros del extremista Partido Pirata de Alemania hicieron aterrizar un dron a pocos metros de Angela Merkel, que estaba dando un discurso, el susto debió ser morrocotudo. Dicen que ella sonrió, posiblemente ignorante de lo que podría haber ocurrido. Saltaron todas las alarmas, pero no…, se trató sólo de un susto y un intento de llamar la atención. Habría bastado con que esta pequeña aeronave portara unos trescientos gramos de explosivo para que aquello hubiera sido una auténtica masacre.

La preocupación es tan intensa y real que la industria busca soluciones urgentes. Varias compañías ya venden soluciones para detectar drones en algunos puntos críticos. Por ahora son muy poco efectivas. Algunas de ellas se basan en detección sonora, lo cual hace difícil su utilización en ciudades, es decir, que en núcleos urbanos son bastante inútiles. Otras utilizan sistemas de radar, poco efectivas también, dado el pequeño tamaño de estas aeronaves. Incluso los sistemas más avanzados de detección por láser no están preparados para esa amenaza, ya que suelen fijar sus objetivos en cosas que generen grandes emisiones de calor y en objetos de mayor tamaño, generalmente metálicos, y un dron no es nada de eso.

Hoy en día, la batalla de la detección es prácticamente imposible. Una sociedad civil en la que se está ensayando con estos pequeños aparatos para que distribuyan pizzas o libros en poblaciones rurales, ¿cómo va a impedir que en la caja que transportan haya otras sorpresas? Hoy por hoy, la solución es difícil.

Más aun, como dije antes, estas aeronaves son simplemente ordenadores voladores, e incluso si desarrolláramos drones para defendernos de los «drones malos» correríamos un riesgo, ya que,

como todo ordenador, incluso los que tienen que defendernos pueden ser hackeados y utilizados en nuestra contra. ¿Ciencia ficción? No. En absoluto. Es una amenaza real y creciente.

En 2012, unos estudiantes de la Universidad de Texas avisaron en repetidas ocasiones a miembros del DHS (Department of Homeland Security) de que los drones con los que se vigilaba la frontera podrían ser hackeados debido a una vulnerabilidad. Tal era la situación que los estudiantes acabaron por realizar una demostración en vivo, tomando el control de los aparatos a su antojo ante la atónita mirada de los oficiales del DHS.

Es sólo cuestión de tiempo que los terroristas empleen estos aparatos de forma creativa. Ni siquiera tienen que innovar demasiado. En la red hay ideas para todo tipo de usos. Por ejemplo, hay vídeos en Youtube de cómo poner en estas aeronaves un arma de fuego del calibre 45, y también de cómo realizar armas con una impresora 3D. De hecho se pueden ver vídeos en los que con la cámara de precisión se hacen demostraciones de tiro con balas de pintura cuya precisión, gracias a las cámaras de alta calidad de las aeronaves, te deja helado y te demuestra que, a día de hoy, no hay salida y pasan muy pocas cosas para las que podrían pasar.

Aunque estos temas se suelen tratar con discreción y se procura que no trasciendan demasiado, se sabe que se han frustrado ya potenciales ataques con drones en numerosos países, como Francia, Estados Unidos, España y otras naciones europeas.

En 2011, el FBI capturó con éxito a un grupo radical vinculado a Al Qaeda y que preparaba un ataque guiado por GPS contra el Capitolio y el Pentágono por medio de drones cargados con explosivo C4. Si hubieran surcado los cielos, la posibilidad de evitarlo era tendente a cero.

Miembros del Estado Islámico usan drones en sus operaciones terroristas y presumen de ello en las redes sociales y en internet. Por ahora son versiones básicas y empleadas fundamentalmente para reconocimiento. El que empiecen a utilizar versiones más modernas que incluyan potencia de fuego es sólo cuestión… de minutos.

No sólo debemos preocuparnos de los terroristas y criminales. Debemos preocuparnos también del uso que de esta tecnología pueden hacer determinados gobiernos. Los drones facilitan guerras rápidas, ataques *lowcost*, en dinero y en coste de vidas humanas, y esos costes, no nos engañemos, ha constituido históricamente un hecho disuasorio por el que muchos países se han pensado muy mucho las consecuencias de sus acciones militares. Ahora, tales costes parecerán menores, y muchos países podrán tomar decisiones bélicas con más alegría.

Hoy, un dron de gama media, que puede tener un coste de entre 1.000 y 6.000 euros, pesa algo menos de dos kilos y tiene capacidad para cargar 500 gramos de explosivo, lo cual lo convierte en el sustituto perfecto de un suicida. Rápido y económico, no hay que lavarle la cabeza ni que prometerle un harén de cientos de vírgenes en el otro mundo, y rara vez fallan. Incluso no hay que pilotarlos remotamente, ya que se puede programar el plan de vuelo previamente.

Ahora, al detectar un zumbido, el presidente Obama a buen seguro ya no mira al cielo con la misma alegría con que lo hacía al empezar su mandato. Éste va a ser uno de los quebraderos de cabeza de las fuerzas y cuerpos de seguridad de los principales países durante la próxima década.

## Como en *Minority Report*, pero sin Tom Cruise

Seguro que has visto la película *Minority Report* (2002). Se trata de una película futurista dirigida por Steven Spielberg y protagonizada por Tom Cruise (bueno, ¡algo malo tenía que tener!).

En 2054, el capitán John Anderton es jefe de la fuerza de policía PreCrimen en Washington D.C. El grupo emplea visiones del futuro que son vistas por los tres «precognitivos». Gracias a ello han frustrado muchos asesinatos antes de que se intentaran perpetrar, logrando así unas tasas de criminalidad bajísimas. Aunque pueda parecerte futurista o visionario, el argumento no es actual, se basa en un relato corto del año 1956, escrito por Philip K. Dick y titulado «El informe de la minoría».

Hoy no contamos (ni parece que podamos hacerlo en los próximos tiempos) con mutantes capaces de predecir el futuro. Pero, pese a que tenemos esa pequeña limitación, y sin necesidad de esperar al año 2054, a día de hoy ya se han creado y se están haciendo intensos avances en las unidades de lo que denominamos como «policía predictiva».

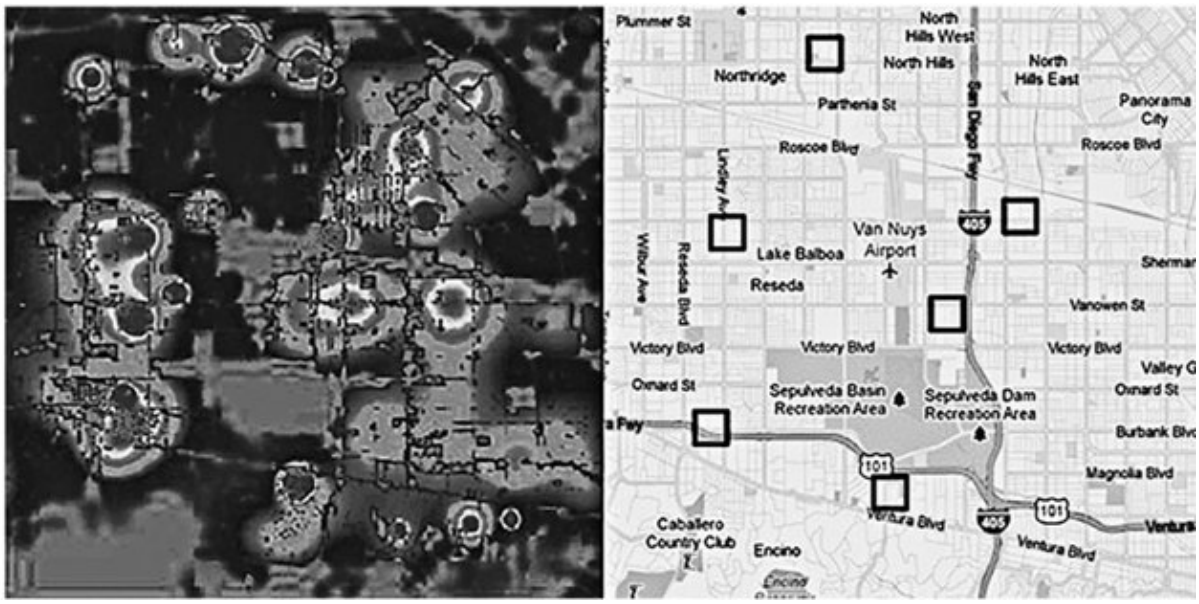
Se llama policía predictiva a la metodología cuyo objetivo es la implantación de estrategias con la habilidad de prevenir la comisión de determinados delitos y de facilitar que las investigaciones sean más efectivas. Los primeros avances en este campo se hicieron en 2010, cuando un grupo de investigadores enumeraron una teoría que considera que se puede determinar la probabilidad de que se cometan delitos, y con la misma exactitud y patrón que hoy en día se predicen los terremotos. Un año después, la revista *Time* determinó que la policía preventiva era uno de los «50 mejores inventos de 2011».

Volviendo a *Minority Report*, hoy, no sólo no tenemos mutantes (¡una pena!), sino que, además, no nos es posible determinar quién va a cometer un asesinato en las próximas horas. Lo que sí nos permite la tecnología es usar los *big data*, la estadística y ciertos algoritmos informáticos para establecer los porcentajes que determinen dónde hay más posibilidades de que se comenta un delito, qué personas tienen mayores opciones de hacerlo y que

grupos o personas podrían ser los objetivos. En manos de la policía, ésta puede ser una herramienta fabulosa. No impedirá el crimen, y ni mucho menos lo erradicará, pero los resultados son alentadores respecto a la reducción de delitos y, porque no decirlo, a la optimización de costos asociados a la persecución del crimen.

Se trata de recopilar datos, analizar y detectar tendencias, establecer posibilidades, analizar patrones de comportamiento, o bien, simplemente, zonas geográficas, momentos del día o fechas del calendario en los que hay más posibilidades de que ocurra algo.

Una *startup* norteamericana llamada PredPol es el máximo exponente en el desarrollo de estos algoritmos, aunque empresas como Motorola, IBM y otras también están trabajando en ello. El *software* de PredPol, instalado ya en cientos de comisarías de Estados Unidos, determina sobre un mapa los puntos calientes estimados para las próximas horas, mediante cuadrados rojos. Así, el *software* avisa de la existencia de entre diez y veinte zonas conflictivas a vigilar predictivamente durante el próximo turno, lo cual permite a los mandos condensar una mayor presencia policial en los mismos.




Fuente: PrePol.

Se trata aún de una utilización de algoritmia y *bigdata* algo rudimentaria, pero empieza a mostrarse efectiva. En 2013, en Santa Cruz (California), durante su primer año de funcionamiento logró unos datos prometedores, ya que redujo los delitos de allanamiento en un 11 por ciento, y los robos, en un 27 por ciento.

Aun así, estos datos no se interpretaron como determinantes, ya que había dudas sobre si la reducción pudiera deberse a una mayor implicación de los agentes, dado que estos sabían que estaban siendo monitoreados y que estaban trabajando bajo la guía de ese *software*. Así que, poco después, se realizó un curioso experimento.

El Departamento de Policía de Los Ángeles (LAPD) intentó demostrar científicamente la eficacia del modelo informático de policía preventiva. Para ello acotaron una zona de la ciudad, llamada Foothill, en la que viven unas 300.000 personas. Diariamente, los jefes de policía distribuían mapas de la ciudad a los oficiales indicando las zonas en las que trabajarían su turno. Unos días eran los mapas tradicionales, otros días eran los mapas que marcaba el algoritmo, pero los agentes nunca sabían a qué modalidad correspondía la tarea diaria.

El resultado del test fue sorprendente. El uso del algoritmo aumentó la tasa de éxito policial. Los días que se utilizaron los «mapas de calor» suministrados por el *software* predictivo, los delitos contra la propiedad disminuyeron un 12 por ciento de media. Sin embargo, los demás días no hubo disminución. Parecía evidente que el modelo era útil.

Singapur tiene en marcha un programa llamado Safe City que da un paso más. No sólo usa *bigdata* y mapas; mediante la utilización en tiempo real de imágenes de cámaras y la capacidad de predicción, el sistema envía automáticamente a la policía a los lugares donde aparentemente se puede producir un delito en los próximos minutos. No tengo datos de la eficacia del sistema, pero, sobre el papel, éste tiene todo el sentido del mundo.

Como sucede con todos lo avances tecnológicos, siempre que llega un modelo que promete mejorar la eficacia del ser humano se entrevé la posibilidad de reducir puestos de trabajo. Esto hace que, de entrada, cada vez que se prueba algo, algunas personas lo vean

como una amenaza y expresen ciertas reticencias. Eso ocurrió con los experimentos de policía predictiva. Hasta que la rotundidad de los datos determino su efectividad, el nuevo sistema tuvo una fuerte oposición por parte de los policías de a pie.

Aun así, estos modelos informáticos están en una fase prometedora, pero todavía inicial, y siempre necesitan del trabajo y la interpretación de un analista. Eso sí, a medida que avancen y se perfeccionen, que mejore la calidad de los datos con los que se alimentan y se incremente la capacidad de procesamiento y comprensión mediante la inteligencia virtual, no hay ninguna duda de que no sólo ahorrarán delitos, sino, para desgracia de algunos, también puestos de trabajo. *C'est la vie.*

Policías de todo el mundo están trabajando ya en estos sistemas, que, como ves, no son tan futuristas como parecían al principio de este apartado. ¡Queremos que haya mutantes!

Eso sí, también el uso y la dependencia de esta tecnología entraña riesgos. Por un lado está el riesgo de recolección de «malos datos», o que incluso la manipulación de los mismos pudiera hacer que el algoritmo no funcionara como debiera. Además, estos sistemas avanzados hacen que, a medio plazo, e irremediablemente, los analistas se relajen y tengan un exceso de confianza en sus resultados. Incluso, rizando el rizo, el hecho de conocer cómo funciona el *software* podría hacer que un experto informático y delincuente en potencia, al analizar los patrones y los resultados a los que llevarán los mismos, decidiera actuar justo de manera ilógica para el sistema, al contrario de las predicciones, de forma que acabaría cometiendo delitos en las zonas donde la policía no estaría vigilante. Eso sería una especie de «agujero negro» en el que el cazador resultaría cazado, ya que la policía actuaría basándose en la expectativa del crimen, mientras que el criminal avanzado lo haría de forma contraria a esa lógica, basándose en la expectativa de la actuación previsible por parte de la policía. Finalmente, el riesgo de que se den «cisnes negros» es también una realidad. Estos patrones son capaces de prever tendencias en función de hechos ya sucedidos, por lo cual la posibilidad de que puedan predecir algo

totalmente nuevo e inesperado (por ejemplo, los atentados del 11-S) es mínima a día de hoy.

En un orden similar de cosas, en Estados Unidos han dado un paso más allá, e incluso están probando escáneres corporales capaces de medir patrones biométricos que delaten quién está a punto de cometer un delito. Al parecer, la teoría se sostiene, y se está investigando mucho en este campo. Se trata de medir determinados patrones, tales como el estrés, el calor corporal, la sudoración, etc., de la misma forma que actúa un detector de mentiras, de modo que, mediante cámaras de seguridad, se puedan así detectar situaciones anómalas que delaten si hay personas que, en apariencia, deberían ser controladas inmediatamente.

Pensarás, esas cosas ¡sólo pasan en Estados Unidos! Y estás en lo cierto, es el mismo país donde se emite un programa de televisión llamado «To Catch a Predator», en el que se ponen cebos a personas mediante perfiles falsos en redes sociales con el fin de atraer y provocar a potenciales acosadores. Si el delirante plan funciona (y parece que lo hace), ponen un anzuelo, el acosador que pica recibe la visita de la policía y de las cámaras de televisión para dejarle en evidencia y ponerle a disposición de la justicia. Esto no tiene nada que ver con la policía preventiva, y de hecho sería ilegal en España y en casi toda Europa. No se puede incitar al delito para provocar una detención. Caricaturizándolo, esto sería como si hiciéramos pasear a un niño de diez años, solo y por una calle oscura, jugando con un fajo de billetes de quinientos euros entre sus manos, mientras esperamos que aparezca alguien que se lo quite para salir de nuestro escondite y detenerle. Para qué vamos a engañarnos, tendríamos a barrios enteros entre rejas. Esto sería una barbaridad, ya que, en España, es ilícito el incitar a la comisión de un delito; y, por añadidura, las fuerzas del orden no pueden crear sin autorización judicial perfiles falsos en internet con la finalidad de atraer delincuentes.

7

# Controla el código y controlarás el mundo

## ¿Y si el futuro fuera como en *Mad Max*?

Quizá sea bueno que, para hablar del futuro, volvamos la vista al pasado y recordemos de nuevo las palabras de Bernard Baruch ante la ONU en 1946: «Hemos de elegir entre la paz y la destrucción del planeta». Como ya señalamos en el Capítulo 5, dedicado a la ciberguerra, la carrera de armamento que tuvo lugar durante la guerra fría puso al mundo al borde del abismo nuclear, y, aunque felizmente no hubo que lamentar la destrucción del planeta, aquellos años los humanos jugamos con fuego, o bueno, mejor dicho, con uranio.

Algunas décadas más tarde, ya en 1979, el director de cine australiano George Miller estrenó la película *Mad Max*, protagonizada por Mel Gibson, la cual tuvo un gran éxito de taquilla y dio origen a una saga de la que, en 2015, se estrenó la última secuela. Pero *Mad Max* fue una película rompedora por muchas más razones, y no sólo por conseguir, con un presupuesto de 375.000 dólares, recaudar más de 100 millones en las salas de cine.

El filme, una obra a caballo entre la ciencia ficción, los *westerns* de acción y las películas de terror, renunciaba a los cánones comerciales que imperaban en Hollywood en la época, no hacía concesiones al público y apostaba decididamente por el feísmo y la violencia de los cómics y la serie B. *Mad Max* era una película distópica que arrancaba en un mundo postapocalíptico. En el universo de Miller, la amenaza de Baruch se había cumplido: los hombres se habían visto en la disyuntiva de elegir entre la paz y la destrucción del planeta, y habían elegido la destrucción del planeta.

El escenario posnuclear que dibuja *Mad Max* es aterrador: las ciudades han desaparecido, las instituciones se han desmoronado, el imperio de la ley ha dado paso al caos, y la justicia ha sucumbido a la ley del más fuerte. Los saqueos se suceden, las bandas de mercenarios desatan el pánico, y los hombres hacen la guerra por los escasos recursos que todavía quedan. El orden tradicional de valores ha saltado por los aires, y la gasolina vale más que la vida.

Por supuesto, *Mad Max* es una película de ciencia ficción, pero no es una película de fantasía. Es decir, dibuja escenarios que no son

reales, pero que podrían serlo, y su verosimilitud se apoya en los fundamentos de las ciencias naturales, físicas o sociales.

La obra de Miller de 1979 especulaba sobre cómo podía ser un mundo posnuclear, todo ello envuelto en un relato de acción. No es el cometido de este libro especular ni, mucho menos, hacer literatura-ficción sobre cuál sería el futuro de nuestro planeta si tuviera lugar una catástrofe sistémica propiciada por la ciberguerra. Sin embargo, sí que podemos utilizar los datos de los que disponemos para tratar de avanzar las consecuencias que podría tener para nuestra forma de vida un fallo tecnológico general.

Sólo así, conociendo los riesgos a los que nos enfrentamos, podremos adoptar la decisión correcta cuando tengamos que volver a enfrentarnos al reto de Baruch: elegir entre la paz o la destrucción del planeta. Sólo así evitaremos que el futuro sea como en *Mad Max*.

## El futuro ya está aquí, y no era exactamente lo que esperábamos

En el libro de Neil Ardley *School, work and play*, publicado en 1981, se explicaba cómo podía ser el mundo del mañana. En uno de sus pasajes, el libro habla del aspecto que puede adoptar el crimen en el futuro. Concretamente, dice así:

> Hay un tipo de crimen que es posible que exista en el futuro, el delito digital. En lugar de asaltar a la gente en las calles o robar casas, los criminales del mañana tratarán de robar el dinero de los bancos y otras organizaciones por medio de ordenadores. El delincuente digital trabaja desde casa, usando su propio ordenador para acceder a las memorias de los ordenadores usados por los bancos y las empresas. El criminal intenta interferir con los ordenadores para transferir dinero al suyo sin que el banco o la empresa sepan que están siendo robados.

Éste era el «mundo de mañana» en 1981, y es el pan nuestro de cada día hoy. Sin embargo, este tipo de crimen, predicho hace más de treinta años, palidece si lo comparamos con la potencia destructora que un ataque digital iniciado por terroristas o por los Estados puede tener dentro de muy poco.

En realidad, uno puede pensar que el dilema de Baruch no debería ser tal, que entre la paz y la destrucción del planeta, todo el mundo elegiría la paz sin pestañear. Que no debería existir ningún obstáculo para que los países y los individuos, en un ejercicio de responsabilidad, acordaran poner freno a la carrera de armamentos digitales.

Efectivamente, lo sensato sería eso. Pero también lo era en 1946, cuando Baruch hizo su ofrecimiento para acabar con la amenaza nuclear. Y la respuesta soviética a ese ofrecimiento fue «no». Los rusos tenían motivos para desconfiar; después de todo, los norteamericanos eran los únicos que habían hecho uso de una bomba atómica hasta entonces. Pero lo fundamental es que no hubo acuerdo.

Ahora vivimos en el siglo XXI, pero es como si nos encontráramos de vuelta en los años cuarenta y tuviéramos que afrontar el mismo

reto. Parece que lo sensato es que elijamos paz frente a destrucción, que antepongamos el bien común a la guerra, pero lo sensato no es lo que ocurre con más frecuencia, como tristemente demuestra la historia.

¿Por qué? Para empezar, porque el bien común no existe. Lo que existen son distintas situaciones en las que siempre hay ganadores y perdedores, y en las que las partes tienen intereses que a menudo son contrapuestos. La guerra horroriza a la mayoría, pero beneficia a unos pocos. Donde unos ven amenazas, otros ven oportunidades. Siempre ha sido así, y también lo es ahora.

Existen incentivos económicos perversos para profundizar en la carrera de armamentos digitales y en la ciberguerra. Mientras la tecnología avanza, el mundo continúa su globalización, las clases medias se desarrollan y nuevos campos de batalla digital aparecen. En este escenario, la inversión necesaria para proteger a las empresas y a los gobiernos crecerá exponencialmente en los próximos años, nuevas asociaciones públicas y privadas florecerán, y las empresas de seguridad y defensa se multiplicarán. Esto, a ojos de un inversor sin demasiados escrúpulos, sólo le dice una cosa: oportunidad.

Hay mucha gente esperando para hacer de la amenaza y del miedo una ingente cantidad de dinero. En Estados Unidos, el mercado de la ciberseguridad movió 65.000 millones de dólares en 2013, y se prevé que esa cifra crezca a un ritmo de entre el 6 por ciento y el 9 por ciento en los próximos cinco años. Eso quiere decir que, en sólo diez años, la ciberseguridad podría representar un mercado de 165.000 millones de dólares anuales en ese país.

## La trampa tecnológica

Y es que internet ofrece muchas ventajas, pero también riesgos. Gracias a la red de redes, todo está interconectado. Empleamos la web para todo: para hacer operaciones bancarias, para buscar recetas de cocina, para almacenar imágenes fotográficas, para conocer al hombre o a la mujer de nuestra vida, para realizar gestiones administrativas, para comprar libros, vender nuestro coche o leer la prensa. Para todo. Y nos conectamos desde nuestros portátiles, nuestro ordenador de sobremesa, nuestro *smartphone*, nuestra tableta, nuestra televisión o nuestra videoconsola.

Las posibilidades que ofrece internet son casi interminables, pero la otra cara de la moneda es que hemos alcanzado un nivel de dependencia digital que nos hace vulnerables. Las centrales eléctricas, el tráfico aéreo, las centralitas de los bomberos y los servicios de emergencia, los ascensores..., todo depende de los ordenadores. Sin darnos cuenta, nos hemos convertido en los arquitectos de una sociedad construida sobre una trampa tecnológica. ¿Y cuál es el plan B de la humanidad si el diseño tecnológico que la sostiene se viniera abajo? Bueno, me temo que no hay plan B.

Como bien señala Marc Goodman en su libro *Future crimes: everything is connected, everyone is vulnerable and what we can do about it* (2015), con internet, el mundo «westfaliano» que imperaba desde el siglo XVII ha desaparecido. La Paz de Westfalia sellada en 1648 dio origen al nacimiento de los Estados nación modernos. En la práctica, esto significaba que los países eran soberanos en sus territorios y que las fronteras dibujaban márgenes de seguridad interior. El tratado de la Paz de Westfalia es uno de los más importantes de la historia de la humanidad, y, sin embargo, hoy carece de sentido.

Carecía de él ya en 1994, cuando Vladimir Levin robó 10,7 millones de dólares al banco estadounidense Citibank sin moverse de su apartamento de San Petersburgo. Levin era un programador informático que, con la ayuda de algunos cómplices, consiguió hackear los sistemas de Citibank y transferir la

mencionada y jugosa suma de dinero a diversas cuentas de Finlandia, Estados Unidos, Holanda, Alemania e Israel.

¿Cómo rayos se aplica el mundo westfaliano a este caso? ¿Qué jurisdicción utilizamos? ¿Qué policía debe perseguir al criminal? ¿La de Estados Unidos, donde se encontraba la víctima (Citibank)? ¿La de San Petersburgo, lugar desde el que se perpetró el crimen? ¿La de los países donde se localizaban las distintas cuentas fraudulentas a las que se transfirió el dinero robado?

Levin nunca entró en Estados Unidos para cometer el delito. No dejó huellas dactilares ni ADN, y no se llevó el dinero con sus manos, lo hizo todo con un clic de ratón. Esto nos da una idea de lo que comentábamos antes: que el mundo westfaliano se ha diluido en un universo sin fronteras ni barreras que separen el mundo digital del mundo real. El mundo digital es parte de la realidad, una realidad cuyo componente digital cada vez adquiere mayor peso sobre el analógico.

## El crimen es como un juego de niños, pero con adultos

El caso Levin es especialmente relevante porque tuvo lugar hace más de veinte años. En el año 2015, las posibilidades delictivas que ofrece internet a criminales, terroristas y Estados son mucho más peligrosas para la sociedad. Cuando los escépticos ponen en duda que un gran ataque digital contra infraestructuras críticas pueda ser llevado a cabo, olvidan que ya hay precedentes.

El caso de un joven hacker llamado Jonathan James (alias c0mrade) es especialmente ilustrativo. El joven fue el primer adolescente en ingresar en prisión con tan sólo dieciséis años de edad. Entre sus «logros» está el de entrar ilegalmente a la Agencia de Defensa para la Reducción de Amenazas (organismo encargado de controlar las amenazas de armas nucleares, biológicas y convencionales) con tan sólo quince años de edad; así como el de entrar en los servidores de la NASA.

Además de obtener 3.300 correos electrónicos del sistema de ordenadores y armas del Pentágono, sus ataques forzaron que la NASA bloqueara los ordenadores de apoyo a la Estación Espacial Internacional durante veintiún días.

Después de ser arrestado, c0mrade se declaró culpable y fue sentenciado a seis meses de prisión; parte de su sentencia incluía la obligación de enviarles sendas cartas al secretario de Defensa de Estados Unidos y al administrador de la NASA para pedirles perdón. Por tratarse de un menor de edad, los cargos no necesariamente reflejan la dimensión de la amenaza a la seguridad nacional que causó c0mrade, pero, si se hubiese tratado de un adulto, la sentencia seguramente hubiera sido mucho más severa.

Al salir de la cárcel, Jonathan James fundó su propia empresa de seguridad informática, como otros tantos. Pero su historia no pudo acabar bien. En 2008, con tan sólo veinticinco años de edad, apareció muerto por herida de bala en su domicilio. Se había suicidado.

Sin embargo, aunque los orígenes de los grandes hackers pueden parecerse un poco al muchacho *geek* que acabamos de describir, los hackers adultos pueden representar una seria amenaza para las

personas, ya sea al servicio de una organización criminal o de un Estado, ya sea actuando en solitario.

También es verdad que el talento de los hackers no tiene por qué ser siempre usado al servicio del crimen, incluso Steve Jobs y Steve Wozniak, que después fundarían Apple, comenzaron su andadura como hackers universitarios en 1971, cuando vendían a los estudiantes unas «cajas azules» que permitían realizar llamadas de larga distancia gratuitas, evitando así los desorbitados costes de estas comunicaciones.

No obstante, esta forma de *hacking* adolescente e inocente pronto fue historia. Hoy ha evolucionado, e internet se ha convertido, entre otras muchas cosas, en el caldo de cultivo del crimen organizado. No solamente encontramos nuevas formas de delitos posibilitados por la tecnología digital, sino que la red de redes ha permitido a las organizaciones criminales tradicionales, las que siempre han operado en «analógico», estar a la última en novedades tecnológicas. Todos, desde la Camorra napolitana a la Yakuza japonesa, pasando por el Estado Islámico, los cárteles colombianos de la droga o la mafia china, cuentan con hackers para competir en el mundo digital, un mundo donde las ganancias son más sencillas, los riesgos más limitados, el anonimato más amplio y la vigilancia policial más difícil.

## Los crímenes de mañana, en los periódicos de ayer

Afirmar que pronto ocurrirán trágicos sucesos facilitados por internet no es jugar a lanzar vaticinios agoreros, sino un hecho respaldado por los datos que tenemos. Los escépticos sobre el impacto que las nuevas tecnologías pueden tener en la guerra, el terrorismo y la delincuencia harían bien en acudir a las hemerotecas de los periódicos: no es que una catástrofe perpetrada con un ordenador no pueda tener lugar, es que se llevan años ensayando.

En 2007, la policía encontró imágenes tomadas con Google Earth de los objetivos que pretendían atacar los terroristas: los tanques de combustible del aeropuerto John F. Kennedy, en Nueva York. Y los criminales no sólo se sirven de las aplicaciones disponibles para el gran público, sino que son *early adopters* de tecnología aplicada a la encriptación y la seguridad de las comunicaciones.

Es el caso de Ramzi Yousef, condenado por ser el ideólogo del primer atentado contra el World Trade Center en 1993, y que utilizaba archivos encriptados para ocultar los detalles de su plan para destruir once aviones civiles estadounidenses. A la policía le llevó más de un año lograr desencriptar el algoritmo de los terroristas, pero, afortunadamente, llegaron a tiempo para evitar que el plan fuera llevado a término. Es muy posible que, en otras ocasiones, las autoridades no puedan adelantarse a las maniobras de los criminales y tengamos que lamentar una enorme tragedia. De hecho, esto ocurrirá; es sólo cuestión de tiempo.

Más recientemente, en abril de 2013, dos hermanos musulmanes atacaron con bombas la maratón popular de Boston, causando la muerte de tres personas y dejando 282 heridos. El terrorista que sobrevivió admitió ante las autoridades que las instrucciones para la fabricación de los explosivos las encontraron en una web de Al Qaeda, concretamente la de la revista digital *Inspire*, donde aparecía un artículo titulado: «Fabrica una bomba en la cocina de tu mamá».

La aplicación de internet y de las nuevas tecnologías a la guerra y la delincuencia son una realidad desde hace años, y en el futuro asistiremos a nuevos episodios de esta forma de ataques, que pueden ser mucho más destructivos. La red se ha convertido en una

suerte de universidad para terroristas y delincuentes, un medio universal y gratuito de escolarizarse en ciencias y tecnología.

## La ilusión democrática de internet

Pero no nos engañemos. No es que internet haya degenerado desde una herramienta democrática de comunicación diseñada para compartir hasta una oscura arma de guerra sucia. Es posible que la mayoría de nosotros acceda a la web para actualizar su estado en Facebook, comentar el último *flame* en Twitter o jugar a Angry Birds. Sin embargo, no debemos olvidar que internet fue desarrollada por la DARPA, es decir, la Defense Advanced Research Projects Agency (Agencia de Proyectos de Investigación Avanzados de Defensa). Vamos, que internet es un invento del Departamento de Defensa de Estados Unidos, creado para asegurar las comunicaciones militares en caso de un ataque nuclear. Internet tiene un origen eminentemente militar, y no social y democrático, como defienden los ciberactivistas y compañía.

El desarrollo tecnológico de las últimas décadas ha hecho posible que internet llegue a ser tal como lo conocemos hoy, facilitando su uso civil, tanto lúdico como aplicado a las actividades cotidianas de las personas. Pero no ha dejado de lado sus raíces bélicas. Paralelamente, los criminales se han adaptado a los nuevos tiempos recurriendo a la imaginación y al ingenio. Y la policía siempre va un paso por detrás de la imaginación y del ingenio. Como escribió el genial escritor británico G. K. Chesterton: «El criminal es el artista creativo, el detective, sólo el crítico».

En internet, esta apreciación del autor de *El hombre que fue jueves* no hace sino subrayarse. Los ciberdelincuentes organizados han adaptado su estrategia al nuevo medio. Los grandes robos de décadas pasadas que dieron origen a películas y narraciones como *El golpe* u *Ocean's eleven* han dado paso a operaciones menos espectaculares, quizá no tan cinematográficas, pero mucho más fructíferas y menos arriesgadas. La consigna criminal de ahora es «robar menos, pero a más». La idea es simple: es mucho más sencillo y discreto robar pequeñas cantidades de dinero a millones de personas que robar sumas millonarias a una sola entidad. Estas operaciones pueden ser automatizadas y sostenidas en el tiempo sin

que, en muchas ocasiones, ni las víctimas ni las autoridades sean conscientes de que el delito se está produciendo.

No obstante, también se dan operaciones delictivas espectaculares. Aunque éstas tienen la desventaja de que son más fácilmente detectadas. En abril de 2015, la línea aérea de bajo coste Ryan Air confirmó que había sufrido una estafa de unos cinco millones de dólares a través de un hackeo en una de sus cuentas y mediante una transferencia electrónica realizada a un banco chino. Así de fácil. Un acceso no autorizado, y el dinero… vuela.

Y este tipo de delitos, aunque muy costosos en términos económicos, cuentan con la ventaja de que no implican violencia física contra las personas. Lamentablemente, las posibilidades tecnológicas hacen que tampoco podamos estar muy tranquilos a este respecto; conforme la tecnología vaya integrándose más y más en nuestras vidas, la trampa tecnológica será mayor, siendo, por tanto, también mayor su amenaza.

## Internet de las cosas

Cuando digo que la tecnología se integrará en nuestras vidas no es una mera forma de hablar. La llamada internet de las cosas, o IoT (*internet of things*), es un concepto que se utiliza para designar la interconexión de los objetos cotidianos con internet. Se trata de tejer una red de objetos integrados en *software*, electrónica, sensores y conexiones para aumentar su utilidad.

En la práctica, la internet de las cosas sería como imaginar que tu despertador está conectado a internet, de tal modo que puede tener acceso a tu agenda y leer tus compromisos y tareas cada día. El despertador podría «saber» a qué hora tienes la primera reunión y, después, comprobar el estado del tráfico. Si el tráfico es fluido, te dejará dormir unos minutos más. Si hay mucho atasco, te despertará antes de la hora prevista para asegurarse de que llegas a tiempo a tu cita. Cuando por fin suene la alarma, tu casa estará también conectada: las luces comenzarán a encenderse suavemente y la calefacción se activará, si así lo tienes programado. O el sistema se encargará de prepararte un baño, y también de hacerte un café. Ni siquiera tendrás que preocuparte por comprobar si tus hijos se han cepillado los dientes: un chip en sus cepillos se chivará a tu *smartphone* con un mensaje. Ya puedes salir de casa. Un momento, ¿dónde has puesto las llaves? No te preocupes, el sensor de tu llavero te permite localizarlas en un santiamén. ¿Suena bien, verdad?

Todo esto no está sacado del filme *Regreso al futuro* ni de ninguna otra película de ciencia ficción, sino que es técnicamente posible hoy en día. En los próximos años iremos completando una progresiva transición desde la conectividad actual hasta la hiperconectividad. En poco tiempo, los objetos se comunicarán unos con otros y tendrán acceso a un montón de procesos e información alojada en la «nube». Tendremos objetos inteligentes y todo será programable e interactivo. Las cosas podrán informarnos de su localización, distancia, velocidad, temperatura, sonido ambiente, visión, aceleración, fuerza, carga, presión, interacciones y un largo etcétera de posibilidades.

En 1999, el concepto de internet de las cosas fue propuesto por el investigador Kevin Ashton en el Instituto Tecnológico de Massachusetts (MIT), donde se realizaban investigaciones en el campo de la identificación por radiofrecuencia en red y las tecnologías de sensores.

La idea es que si los libros, los termostatos, los refrigeradores, la paquetería, las lámparas, los botiquines, las partes automotrices, etc. estuvieran conectados a internet y equipados con dispositivos de identificación, no existirían, en teoría, cosas agotadas en las existencias o medicinas no disponibles o caducadas. Sabríamos exactamente la ubicación de todos los objetos, conoceríamos cómo se consumen y compran productos en todo el mundo; así, las eternas preguntas de «¿he apagado el fuego?» o «¿he cogido las llaves?» ya no tendrían sentido; el extravío sería cosa del pasado y sabríamos qué está encendido o apagado en todo momento.

Por si fuera poco, internet hará posible el control remoto de cualquier objeto sobre la Tierra. En resumidas cuentas, los expertos calculan que la internet de las cosas tendrá un impacto sobre la vida de las personas entre cinco y diez veces mayor que el de la propia internet. Cuando la IoT se desarrolle plenamente, la distinción entre el mundo virtual y el mundo físico se habrá evaporado para siempre, los dos mundos se habrán fundido en uno solo de forma indisoluble.

## Los riesgos de la hiperconectividad

No cabe duda de que el desarrollo tecnológico nos hace la vida más fácil y supone un buen número de avances para las personas. Sin embargo, no está exento de riesgos. Cuanto más interconectamos todo, cuanto mayor es nuestra dependencia de la tecnología para vivir, mayor es la trampa tecnológica de la que hablábamos antes.

Al incrementar los niveles de información y la conectividad de nuestros objetos cotidianos, estaremos poniendo al descubierto un montón de información muy valiosa sobre nosotros mismos. Todo lo que hacemos en nuestras casas, trabajos, coches, escuelas, comunidades y tiempo libre será susceptible de ser monitoreado por la tecnología, y, después, convenientemente reportado a sus empresas fabricantes.

Por supuesto, toda esa información será vendida a los publicistas y a los gobiernos. Esto no es una novedad, pues ya hemos visto qué sucede con Facebook, Google o Apple. Estamos en un escenario paradisíaco para estas compañías, y, en consecuencia, para el Gobierno de Estados Unidos y sus animosos chicos de la NSA. Hasta ahora, siempre hemos tenido la opción de cerrar nuestra sesión de Facebook y darnos de baja del mundo digital, pero eso será imposible cuando la hiperconectividad culmine y el mundo analógico y digital sean uno solo.

La presión del nuevo Gran Hermano puede ser incluso mayor que la que describiera George Orwell en *1984*. En poco tiempo, tu reloj inteligente podrá informar a tu aseguradora de salud de que estás haciendo poco ejercicio, tu coche se chivará al seguro de tu coche de que te gusta pisar el acelerador más de la cuenta, y tu basura le contará al ayuntamiento que no reciclas correctamente. ¿Ciencia ficción? Nada de eso, ¡ya está pasando!

Existen compañías de seguros para automóviles, como Progressive, que ofrecen descuentos personalizados en función de tus hábitos de conducción. ¿Y cómo conocen tus hábitos de conducción? Muy sencillo: todo lo que el cliente tiene que hacer para obtener el mayor descuento es aceptar la instalación de una pequeña caja negra en sus vehículos para analizar el uso que hacen

de los frenos, el acelerador y los kilómetros que recorren. No es difícil aventurar que aquellos que se nieguen a instalar los dispositivos controladores tendrán que afrontar una póliza muy costosa, por lo que, en la práctica, la aplicación de estos artefactos se tornará obligatoria a largo plazo.

Y la publicidad personalizada que ya aparece hoy en tu Facebook estará por todas partes. Tu nevera sabrá qué productos consumes más, y te mostrará una pantalla con publicidad ajustada a tus hábitos de consumo cada vez que la abras. Las marcas competirán por obtener esa información para ofrecerte alternativas e intentar que no pidas productos de la competencia. Google ya ha anunciado su intención de colocar publicidad en frigoríficos, relojes, termostatos, gafas o salpicaderos de coche.

## Libertad vigilada

Y todo es susceptible de ir más lejos. Los dispositivos de localización se han vuelto muy populares entre los propietarios de mascotas preocupados por una posible pérdida de sus amigos peludos. Pero no sólo son apreciados por aquellos que tienen compañeros de cuatro patas. Las pulseras localizadoras son cada vez más frecuentes entre los niños. En algunos lugares de Estados Unidos ya es obligatorio que los menores estén «etiquetados». Así sucede en el colegio de Contra, en California, donde los preescolares deben vestir unas camisetas con tecnología de localización para permitir a los profesores saber dónde está cada alumno en cada momento. Según la escuela, esto les ahorra unas tres mil horas de trabajo al año, y seguro que también les evita más de un susto.

Los detractores de estas aplicaciones alegan que los instrumentos de localización anulan la libertad de quienes los llevan, obligándoles a vivir en una «jaula» (de hecho, su principal uso hasta ahora había sido el de monitorear a presos en libertad vigilada). Sin embargo, también hay expertos que las defienden. Dispositivos como estos permiten identificar mejor a los alumnos que se mueven más, ayudando al diagnóstico precoz de trastornos como la hiperactividad y otras alteraciones de la conducta.

Sin embargo, quien ose rebelarse contra la imposición de la vigilancia podría verse envuelto en problemas. Es lo que le pasó a Andrea Hernández, una estudiante de San Antonio que fue suspendida después de negarse a llevar la identificación requerida en el campus.

Y la obsesión por la localización no sólo se limita a los menores de edad. Las empresas ya se frotan las manos con la posibilidad de monitorear el tiempo que sus empleados se toman para comer, para ir al baño o para realizar tareas. Pueden conocer el número de palabras que teclean, cuántas llamadas atienden, el tiempo que pasan fuera de su escritorio, hasta aspectos como la respiración o el movimiento de los ojos, conocer quién pasa tiempo con quién y mucha más información. Piénsalo.

Otra cosa llamativa es que ya se monitorean los patrones de consumo para detectar conductas irregulares. Por ejemplo, han sido dictadas órdenes de registro y detención de sospechosos de cultivar marihuana únicamente apoyadas en una factura de la luz demasiado alta (los cultivos interiores de marihuana necesitan mucha luz). Muy pronto, los policías podrán extraer información de tu frigorífico, tu reloj inteligente o tu lavadora si han «presenciado» un crimen. Esta idea será suficientemente disuasoria en el futuro si estabas pensando en hacer algo raro.

## Póntelo, pónselo

El internet de las cosas supone un gran avance tecnológico que no está exento de riesgos, pero la innovación todavía puede ir más allá. Es el caso de la tecnología *wearable* o «ponible», que en los últimos años ha experimentado un *boom* en Estados Unidos. La tecnología ponible va un paso más allá: en lugar de ser la internet de las cosas, puede considerarse como la internet de las personas. Son artefactos que se llevan en el cuerpo, bien sobre él, bien dentro de él, y que están conectados a la red.

En 2014 se vendieron más de cien millones de *wearables* en todo el mundo, y se espera que la cifra ascienda hasta los 485 millones de unidades en 2018. El número y variedad de estos productos se ha multiplicado en muy poco tiempo: desde pulseras de actividad como Fitbit Flex, Nike Fuelband o Jawbone UP, hasta relojes inteligentes como Pebble, Samsung Galaxy Gear o Apple Watch, pasando por gafas, como las Google Glass, y otros dispositivos.

La mayoría de estos artefactos se sincronizan automáticamente con el teléfono móvil de su propietario, vía wifi o bluetooth, y monitorean su actividad física para mejorar su rendimiento y ayudarle a alcanzar sus objetivos físicos. El problema de estos populares instrumentos es que son fácilmente hackeables. Además, una de las últimas tendencias en tecnología ponible es la de integrar cámaras en los dispositivos, lo cual ha despertado no pocos recelos. Las Google Glass han sido prohibidas en numerosos lugares públicos, como eventos deportivos, salas de cine, bares, restaurantes, clubes de *striptease*, casinos, hospitales, conciertos, vestuarios de gimnasio o teatros, por miedo a que se cometan robos, espionaje o piratería con ellas.

Además, las Google Glass han sido víctima de los hackers incluso antes de que hubieran salido al mercado. Cuando las gafas son hackeadas, las imágenes y los sonidos que reciben son retransmitidas en tiempo real al responsable del ataque, incluyendo la información de la cuenta del usuario y su contraseña, sin que su propietario sea consciente de nada.

## Los rompecorazones (literalmente)

Pero los *wearables* no sólo se ponen sobre el cuerpo, sino también dentro de él. Millones de personas en todo el mundo llevan Dispositivos Médicos Implantables (IMD, por sus siglas en inglés), y, sólo en Estados Unidos, unas trescientas mil personas reciben uno de estos implantes cada año.

En 2009, a una paciente de Roslyn (Nueva York) le fue colocado el primer marcapasos con wifi. Gracias a esta nueva tecnología, los médicos pueden conocer en tiempo real las constantes vitales de los pacientes, ayudando a prevenir crisis cardiacas y reduciendo considerablemente el número de visitas a las consultas de cardiología. A este hito de la medicina hay que sumar otra serie de dispositivos que se comunican por wifi o bluetooth, tales como implantes cocleares, bombas de insulina o estimulantes neuronales.

El problema, claro está, es que estos artefactos también son susceptibles de ser manipulados por hackers. El Departamento de Seguridad Nacional de Estados Unidos ya advirtió, en 2013, de que unos trescientos dispositivos de cuarenta fabricantes diferentes tenían vulnerabilidades que podían ser fácilmente explotadas por hackers malintencionados. Basta decir que no es lo mismo tener un virus en tu *smartphone* (que en la mayoría de los casos se puede eliminar aplicando un antivirus adecuado, o si es un tema muy radical tirando el móvil a la basura) que en un marcapasos o un desfibrilador automático implantado (cuyo reseteo o reemplazo supone abrirle quirúrgicamente el pecho al paciente). Este escenario nos lleva exponencialmente al pánico, y, por tanto, a la Disneylandia de los terroristas.

El caso de los marcapasos y los desfibriladores hiperconectados es especialmente preocupante si tenemos en cuenta que los hackers podrían conseguir no sólo que el marcapasos o el desfibrilador dejaran de funcionar, sino inducir en ellos comportamientos erráticos o enviar descargas eléctricas que podrían tener una consecuencia fatal para la vida del paciente.

Estas posibilidades ya han sido abordadas incluso en la popular serie de televisión norteamericana *Homeland*, en la que, en uno de

sus episodios de 2013, el vicepresidente de Estados Unidos era víctima de un ataque terrorista perpetrado de forma inalámbrica contra su marcapasos. A la emisión de este capítulo siguió la polémica y la especulación sobre la posibilidad de que el ataque descrito por la serie pudiera ocurrir en la vida real. El experto Barnaby Jack afirmó entonces que era posible alterar el *software* de los marcapasos, modificando sus ajustes y parámetros, y enviando descargas eléctricas de alto voltaje.

Es decir, que, una vez más, no estamos hablando de ciencia ficción. De hecho, poco después de este debate, el exvicepresidente estadounidense Dick Cheney decidió inhabilitar todas las opciones de conexión remota de su marcapasos por seguridad. Para ello, alertado por su servicio de seguridad, se sometió a una operación de corazón, temeroso ante la posibilidad de que pudiera ser objeto de un ataque terrorista que accediera a su marcapasos y le provocara la muerte.

Tan sólo en Estados Unidos hay unas setenta mil personas con marcapasos conectados a internet. Lo sepan o no, están corriendo un riesgo.

Si el *hacking* de tecnología ponible y objetos hiperconectados a través de la internet de las cosas ya es posible y ya sucede en nuestros días, no es difícil aventurar que en el futuro aumentarán exponencialmente los delitos y crímenes relacionados con ello, especialmente a medida que la tecnología progrese y el mercado de objetos inteligentes y conectados vaya creciendo.

## Bienvenidos a Gattaca

En 1997, el director Andrew Niccol estrenó la película de ciencia ficción *Gattaca*. Protagonizada por Ethan Hawke, Uma Thurman y Jude Law, *Gattaca,* inspirada en el libro de Aldous Huxley *Un mundo feliz*, describía un futuro no demasiado lejano en el que la manipulación genética y los controles biométricos están a la orden del día.

Las parejas que aspiran a ser padres pueden intervenir directamente sobre el proceso de concepción de sus hijos, seleccionando todas sus características genéticas. Quienes no son concebidos por medio de la ingeniería genética son considerados «inválidos», y se les empuja a los márgenes de la sociedad.

Vincent, el protagonista, nunca podrá cumplir su sueño de viajar al espacio, porque sus padres decidieron que querían que su nacimiento fuera fruto de un acto de amor, y renunciaron a las eugenésicas prácticas popularizadas. Sin embargo, la determinación de Vincent por alcanzar su sueño es tan firme que nada se le podrá poner por delante. Logrará burlar todos los controles biométricos (los de ADN, geometría facial, huellas dactilares, análisis del iris y reconocimiento de voz) para intercambiar su identidad con la de un individuo «válido», que ha quedado paralítico tras sufrir un accidente, y, así, poder ser seleccionado para formar parte de una misión que viajará al planeta Titán.

Pues bien, parece que el futuro que anunciaba *Gattaca* ya ha llegado.

Aparentemente, estos avances técnicos deberían ser positivos, al fin y al cabo, las huellas dactilares son únicas e intransferibles y, por tanto, imposibles de falsificar. ¿Imposible? Lo cierto es que no parece haber nada imposible para el crimen organizado.

Como ya conté en un capítulo anterior, la mafia malasia fue la primera en lograr burlar los controles de reconocimiento dactilar para robar los Mercedes clase S que incorporaban esta tecnología. ¿Cómo lo conseguían? Muy fácil: cortándoles los dedos a sus propietarios con machetes. No es muy sofisticado, pero era un método barato y efectivo.

Sin embargo, los hackers informáticos han conseguido burlar los escáneres biométricos de modo mucho más limpio y menos violento que los gánsteres malasios. De hecho, ya hay decenas de vídeos en Youtube que explican cómo hacerlo.

Tsutomu Matsumoto, investigador sobre seguridad en la Universidad Nacional de Yokohama, ha diseñado un método que le permite tomar una fotografía de una huella dactilar y recrearla en una gelatina. Y otros hackers han conseguido reproducir huellas dactilares por medio de moldes de plastilina que consiguen burlar más del 90 por ciento de los escáneres biométricos.

Vale la pena recordar otro caso que ya mencioné también antes… En 2008, el entonces ministro de Interior de Alemania, Wolfgang Schäuble, se mostró como un entusiasta partidario de la adopción de los sistemas de reconocimiento dactilar. Un grupo de hackers del Chaos Computer Club decidió entonces darle una lección de seguridad informática al ingenuo ministro: tomaron sus huellas de un vaso de agua después de que Schäuble impartiera una conferencia en una universidad pública, las copiaron y las reprodujeron con un molde de plástico. «Sólo» hicieron 4.000 copias, que después fueron distribuidas con la revista del club, la cual también contenía un artículo en el que se animaba a los lectores a que hicieran uso de esas huellas para suplantar el ministro.

Los hackers habían demostrado que, en contra de lo que muchos creían, las huellas dactilares sí podían ser robadas. Pero, además, resulta que las huellas dactilares tampoco son inmutables como pensábamos. Recordemos un ejemplo ya citado anteriormente… En 2009, Lin Ring, una mujer china de veintisiete años de edad, se sometió a una cirugía para cambiar sus huellas dactilares y así poder burlar los controles biométricos de inmigración en un aeropuerto de Japón. La mujer había sido repatriada con anterioridad, y tenía prohibido regresar al país nipón, de modo que pagó 15.000 dólares para poder intercambiar las huellas de su mano derecha con las de la izquierda, y burlar así la sanción. La argucia funcionó, y la mujer pudo por fin entrar en Japón. Aunque no duró mucho su alegría: despertó las sospechas de la policía cuando trató de casarse con un

japonés mucho mayor que ella, y las autoridades repararon en las extrañas cicatrices circulares alrededor de sus dedos. Al parecer, el de Lin Ring no es un caso aislado, y, ese mismo año, la policía arrestó a otras nueve personas más por fraude biométrico.

## Por tu cara bonita

Los escáneres biométricos, como ya dijimos también en un capítulo anterior, no se ciñen únicamente a dispositivos de reconocimiento de huellas dactilares. En los últimos años la tecnología ha conseguido aplicar estas técnicas al reconocimiento facial. Estos escáneres permiten identificar tus facciones, midiendo la distancia entre tus ojos, tu nariz, tus orejas y tus labios. De este modo, no sólo se puede identificar a un individuo por medio de técnicas biométricas, sino que es posible realizar un perfil de cualquiera a través de su sexo, edad, raza y etnia.

A los expertos en marketing ya se les hace la boca agua pensando en que van a poder disponer de todos estos datos para millones de personas, lo cual les permitiría ajustar la publicidad a cada tipo de individuo. Pero ésta no es la única utilidad que tienen estos dispositivos. En algunas tiendas, los reconocimientos faciales se utilizan para identificar a conocidos ladrones y poner en alerta a los dependientes cuando uno de ellos entra en el establecimiento. Y en la cadena hotelera Hilton se usan para reconocer a los clientes (especialmente a los VIP) y poder saludarles por su nombre.

Los dispositivos biométricos faciales también se han comenzado a hacer populares en bares y discotecas. Y no están ahí por tu seguridad, para evitar que te roben. En lugares como Austin, en Texas, algunos pubs utilizan esta tecnología para enviar las imágenes que graba la cámara a los usuarios de la aplicación SceneTap, que te permite ver en tiempo real cuál es el ambiente en los bares. Así, la aplicación manda fotos y estadísticas de la gente que hay en los locales: si hay muchas personas o está casi vacío, si hay muchas mujeres o muy pocas (esto es importante para algunos seudoligones profesionales), si la media de edad de los asistentes el alta o baja, etcétera.

La precisión de los sistemas de reconocimiento facial ha mejorado muchísimo en los últimos años, y en 2014 ya alcanzaba una eficacia del 98 por ciento, 20 puntos más que diez años antes. Este avance tecnológico ha despertado el interés de los gigantes de internet. Google y Apple han realizado costosas inversiones en estas

herramientas, aunque quien se lleva la palma es Facebook. La empresa creada por Mark Zuckerberg compró en 2012 la *startup* israelí Face.com por cerca de cien millones de dólares. Face.com permitió a Facebook, a través de sus algoritmos biométricos, mejorar sus sugerencias de etiquetas en fotografías, en las que llevaba años trabajando. El resultado es que Facebook es hoy el mayor propietario de datos biométricos del mundo, por encima de cualquier empresa o Gobierno.

Bueno, quizá no más que cualquier Gobierno, pues gracias a Snowden sabemos que la NSA norteamericana tiene acceso a los datos personales de Facebook, así como a los de Google, Yahoo!, Apple y otros gigantes de internet. Caricaturizando la situación, podríamos decir algo así como que Facebook es el «ministerio de información biométrica» del Gobierno de Estados Unidos, lo que convertiría a Mark Zuckerberg en algo así como en el secretario de Estado.

A pesar del indudable abanico de oportunidades que ofrece esta nueva tecnología, en el futuro, los datos biométricos pueden ser fuente de disputas y conflictos, y pueden suponer un peligro si se hallan en manos equivocadas.

Dentro de poco veremos esta tecnología aplicada a la guerra convencional, con cámaras instaladas en drones que pueden identificar a un objetivo por medio de sistemas biométricos, apuntarlo y asesinarlo de forma autónoma, sin necesidad de que ninguna persona intervenga o apriete el gatillo.

De hecho, el uso de la tecnología de reconocimiento facial para fines ilícitos ya ha comenzado. En 2011, un individuo despertó la atención de las autoridades australianas cuando se encontraba disparando fotos con una cámara profesional con teleobjetivo durante una ceremonia de graduación de nuevos policías. Los agentes descubrieron que el tipo en cuestión era miembro de una banda de moteros relacionada con el crimen organizado, y que estaba recopilando imágenes para un archivo fotográfico de reconocimiento facial de policías. Con ello pretendían identificar al mayor número de agentes posible para poner en guardia a los integrantes de la banda ante posibles infiltraciones policiales.

Y el uso de tecnología biométrica no sólo puede tener graves implicaciones para los policías que se encuentran trabajando en una investigación como infiltrados. También puede ser muy problemático en programas de reubicación de testigos y, en general, para cualquiera que por razones de seguridad quiera dejar atrás su pasado.

## Biohacking

Y el horizonte a medio plazo es menos alentador aún. Los sistemas operativos de los ordenadores del mundo, compuestos por ceros y unos, llevan décadas siendo atacados. Pero hay otro código fuente que espera ser vulnerado.

El avance de la biotecnología es una de las grandes esperanzas de la salud y de la calidad de vida para los próximos años. Se trata de la rama de tecnología más potente y con mayor potencial de crecimiento. Si me dijeran que en la próxima década se creará desde cero un nuevo gigante tecnológico como Google, Apple, Amazon, Facebook o Microsoft, apostaría que será una empresa biotecnológica o una dedicada a la robótica. Veremos si me equivoco…, eso sí, en diez años.

El poder potencial de esta ciencia nos lleva a revolucionar la vida tal y como la conocemos, como, por ejemplo, con el reemplazo de los combustibles fósiles que se agotan rápidamente en nuestro planeta.

Se espera que en pocos años podamos, por ejemplo, retocar la genética de los niños modificando su ADN para eliminar determinadas enfermedades de carácter genético que actuarían a medio y largo plazo como bombas de relojería en su organismo.

Se estima que cerca de veinte millones de personas mueren cada año por enfermedades que se podrían haber previsto y prevenido si se hubieran conocido sus ADN y sus riesgos vitales.

Se podrán erradicar decenas de enfermedades que, en un alto porcentaje, tienen origen en nuestros genes. Del mismo modo que se podrán eliminar algunos genes que representen un riesgo, se podrán potenciar otros, como, por ejemplo, los que mejoran nuestra inteligencia.

La biotecnología puede prevenir futuros males, pero también entraña sus riesgos. En una charla ofrecida a principios de 2015, Bill Gates, fundador de Microsoft, lanzó un mensaje preocupante que me provocó una enorme reflexión. Si en la próxima década ocurre algo que mate a más de diez millones de personas en el mundo, posiblemente no será una guerra ni un desastre nuclear, y, desde

luego, no será el hambre… Será una pandemia originada por algún virus; y hay muchas posibilidades de que ese virus no sea natural, sino una creación sintética, es decir, un virus «fabricado» en un laboratorio. Con ello me refiero a la utilización de la biología sintética con fines terroristas.

Hemos vivido una enorme alerta en determinados países africanos con el Ébola. Han fallecido unas doce mil personas. La cifra es enorme, desde luego, pero aunque nos pueda asustar su carácter es limitado. La diferencia entre el terrible virus del Ébola, y el de la gripe española en 1918 es que la propagación de este último fue por el aire. Por eso se produjeron en todos los continentes hasta 33 millones de muertos en 18 meses.

Hoy, la ciencia nos acerca a poder modificar un virus terrible como el del Ébola en un laboratorio, y también a lograr que pueda transmitirse por el aire, lo cual, en un mundo mucho más interconectado que a principios del siglo XX, tendría unas consecuencias devastadoras. Para paliar esta posibilidad existe una vieja reclamación que pide que los servicios médicos de todo el mundo dispongan, al igual que ocurre en el ámbito militar, de un sistema de intervención temprana a escala mundial, similar al de la OTAN, para que, en caso de producirse una amenaza de pandemia, se pueda actuar con contundencia, medios y rapidez en cualquier parte del mundo.

Y así llegamos al *biohacking*, una metodología que apuesta por mezclar los conceptos biotecnológicos que están cada vez más a nuestro alcance, sacándolos del laboratorio con criterios de la ética hacker. Se trata de buscar cómo aprovechar toda esa información que ahora mismo está en los laboratorios, pero que no se emplea en la calle, en el día a día de las personas.

Hoy, empezamos a tener *wearables* alrededor nuestro. Se comunican generalmente con nuestro teléfono móvil, y nos dicen cuánto hemos caminado, si nos sube la presión arterial, etc. Hay investigadores que consideran que la evolución lógica es que esos *wearables* sean implantes corporales, pequeños chips con biosensores que, desde nuestro interior, podrán, por ejemplo, medir nuestra glucosa en la sangre y avisarnos con algún pitido

estruendoso en nuestro teléfono móvil, como si nos dijera: «¡Eh!, no comas más pastel de chocolate. Tu nivel de glucosa en sangre es ya muy elevado, y recuerda que eres diabético!».

De hecho, se espera que estos mismos dispositivos puedan segregar determinadas sustancias en caso de necesidad. Por ejemplo, si la presión arterial se dispara, no sólo te avisarán de que estás a punto de tener un ataque al corazón, sino que podrían liberar una dosis de nitroglicerina en tu organismo.

Venimos de la época del ordenador personal, y ahora estaríamos adentrándonos en la era de la biotecnología personal.

Esto es el futuro de la medicina personal, pero también entraña todo tipo de riesgos. El hackeo de estos biosensores o la implantación de otros «infectados» harían que no sólo tuviéramos que utilizar un antivirus en nuestro ordenador o teléfono móvil, sino también en nuestro organismo. Eso sí, todo esto que está por llegar no parece tan inminente como otras muchas cosas de las que hablamos en este libro.

## ¿*Smartcities* o ciudades no tan inteligentes?

Si tenemos objetos hiperconectados gracias a la internet de las cosas, tenemos *wearables* que nos permiten llevar la conexión inalámbrica sobre el cuerpo de las personas y tenemos tecnología que nos permite integrar nuestros propios organismos con la red, el envoltorio de todo ello, las ciudades, también habrá de ser inteligente por fuerza en un futuro próximo.

Como afirmó Goodman: «La internet de las cosas tiene todo el potencial para transformar las ciudades en ecosistemas vivos, que respiran, de ambiente inteligente y sensores conectados, que pueden mejorar ampliamente la calidad de vida de sus habitantes. En la utópica visión de las ciudades inteligentes, los contenedores de basura con sensores integrados notificarán a los recolectores de basura que están llenos, siendo enviado inmediatamente el camión equipado con GPS más cercano para recogerla. El número creciente de "redes municipales de sensores" puede medir la contaminación emitida por los edificios, la calidad del aire en un bloque particular o el número de peatones que camina por una determinada calle, creando el primer "Fitbit para la ciudad". Mejores sensores en la iluminación de nuestras ciudades se traducirán en que los ayuntamientos serán capaces de proveer el nivel de luz exactamente necesario, correctamente ajustado a la hora del día, la estación del año, las condiciones climáticas, etc., reduciendo así los costes de energía hasta en un 30 por ciento».

Por supuesto, ése es el lado amable de la historia. La otra cara es que la creciente integración de los objetos y las personas a través de la internet de las cosas puede tener consecuencias muy desagradables, tanto sobre nuestra privacidad como sobre nuestra seguridad. Ya hemos hablado de cómo la tecnología nos puede llevar a una situación orwelliana en la que nuestra intimidad desaparezca definitivamente y vivamos bajo un estado de vigilancia constante.

Pero, además de ello, el hecho de tener nuestras ciudades, y con ellas, nuestros coches, cafeteras, edificios, teléfonos móviles, ascensores, lavaplatos, juguetes, y un sinfín de objetos conectados

unos con otros, abre la puerta para que los criminales aprovechen todas esas vulnerabilidades en contra de nosotros.

De hecho, ya ha empezado a suceder. Un argentino llamado César Cerrudo consiguió hackear los sistemas de regulación del tráfico de Manhattan. Alteró los semáforos de forma que se produjo un caos circulatorio importante. Es obvio que las consecuencias de este tipo de manipulación podrían haber sido mucho menos benignas si fueran llevadas a cabo por terroristas u otros criminales más peligrosos.

Y no sólo los semáforos son susceptibles de ser hackeados. En el futuro, cualquier cosa podrá ser objeto de manipulación por parte de hackers informáticos: desde los ascensores de un edificio hasta sus sistemas de ventilación, pasando por las cerraduras, la iluminación, los túneles, los puentes, los sistemas de tratamiento de aguas, las plantas eléctricas, y cualquier otra infraestructura crítica, con consecuencias que podrían ser fatales.

Desde el 11 de septiembre de 2001, todos sabemos lo vulnerables y críticos que pueden resultar los aviones en los atentados terroristas. ¿Puede un avión ser atacado y manipulado informáticamente? La respuesta, a estas alturas, ya la conoces o la puedes intuir.

En marzo de 2015 ocurrió un terrible suceso que todos recordamos. Un avión Airbus 320 que había partido de España se estrellaba en los Alpes, con el resultado de 150 personas muertas. Poco después se confirmaban las peores noticias. Había sido un atentado por parte del imbécil del copiloto del avión, que decidió acabar con su vida y, de paso, llevarse a muchos otros inocentes por delante.

Pocos días después del suceso empezó un intenso debate que me llenó de pavor. Determinados medios pedían que, en casos similares, la torre de control pudiera tomar de forma remota el control del aparato, inhabilitando los controles físicos y haciéndolo aterrizar. Sentí un intenso frío recorrer mi cuerpo sólo de pensarlo. Si cualquier avión pudiera ser controlado de forma remota por motivos de seguridad inutilizando sus mandos, tendríamos cientos de terroristas a nivel global buscando la forma de poder acceder y

tomar control de los mismos. Es simple, si es factible hacerlo desde una torre de control, un terrorista con suficientes credenciales podría hacerlo del mismo modo. El escenario sería lo tan aterrador como para que yo me planteara no volver a volar en un bicho de estos en lo sucesivo…

Repito: esto no es ciencia ficción. Ya es posible. En 2014, un investigador de seguridad fue capaz de hackear y tomar el control de la planta eléctrica que surtía de energía a Ettlingen, una ciudad de unos cuarenta mil habitantes en Alemania. Si él fue capaz, siendo una única persona y sin demasiados medios ni recursos, también otros hackers organizados, con medios y una motivación podrían comprometer las infraestructuras críticas de las grandes ciudades. De hecho, eso se va a producir con consecuencias graves en el futuro irremediablemente.

Hoy también piensan que esto es muy real los 140 pasajeros de un avión del Gobierno polaco que, en junio de 2015, abortó con un terrible frenazo el despegue al detectar los pilotos que los sistemas habían sido comprometidos. La maniobra despertó el pánico de la delegación de diputados polacos que se encontraba a bordo, incluido el presidente del Parlamento polaco, Radoslaw Sikorski.

Jerzy Wenderlich, uno de los vicepresidentes del Parlamento polaco que viajaba en el avión, explicó a los medios que la aeronave estaba en la pista de despegue a alta velocidad cuando los pilotos de repente frenaron «de una manera terroríficamente repentina». Los pilotos dijeron a los pasajeros que había un problema con el sistema de navegación. Poco después trascendió que un ataque informático había dejado los aviones de la línea aérea polaca LOT sin operatividad para poder utilizar los planes de vuelo.

El sistema informático de LOT sufrió un ataque que lo dejó incapaz de enviar los planes de vuelo de la aeronave antes del despegue. Sin este documento, que detalla la ruta, el tiempo y otra información importante, los aviones no eran capaces de volar. Para evitar males mayores se abortó el despegue en el último suspiro. Si no hubiera llegado a hacerse así, todo podría haber acabado en una tragedia.

Los aviones cada vez están más conectados. Esto pone en riesgo su seguridad, por más que aumente el confort, las posibilidades de aprovechar el tiempo y la diversión durante el vuelo. Un informe de la Oficina de Responsabilidad Gubernamental de Estados Unidos, publicado en 2015, pone de relieve el riesgo de que todos los sistemas de un avión puedan verse comprometidos en vuelo si su wifi es hackeado. Y los malos no ahorrarán recursos en intentarlo.

## Las dos caras del progreso

En definitiva, la tecnología es como aquel personaje de Batman, Dos Caras. La mitad de su rostro nos hace la vida más fácil y nos proporciona una ingente cantidad de ventajas. La otra mitad es más oscura. Como apuntó el exdirector de la CIA David Petraeus, la internet de las cosas transformará el mercado negro. Además, mientras en el viejo modelo de espionaje corporativo y gubernamental las escuchas se realizaban colocando un pequeño dispositivo oculto en la habitación para grabar conversaciones, ahora es tu propio *smartphone* o tu propio wifi el que le proporciona la información al Gobierno o a las empresas privadas en tiempo real.

Bueno, a las empresas, a los gobiernos y a todos los delincuentes interesados en hackear tus comunicaciones.

Los malos empiezan a ser creativos, son *early adopters* y aprenden rápidamente. Es muy entretenido hacer volar un dron y tomar fotografías. ¡Quién nos lo hubiera dicho hace cinco o diez años! Pero eso también debió pensar un miembro de Al Qaeda detenido en Estados Unidos cuando planeaba usar drones de tipo cuadricóptero, capaces de volar a alta velocidad, para cargarlos de explosivos C4 y enviarlos a estrellarse contra diferentes edificios federales.

Visto lo visto, ¿deberíamos impedir el vuelo de drones cerca de centrales nucleares, presas y demás infraestructuras críticas? Suena razonable, ¿verdad? Y la pregunta del millón, ¿cómo vamos a hacerlo?, ¿con qué medios, recursos y tecnología? Es una obviedad que los delincuentes llevan ventaja, y no están pasando más cosas aún simplemente por una cuestión de velocidad y tiempo.

Los controles de armas son muy rigurosos, y se han mostrado muy efectivos en algunas instalaciones oficiales. Esos arcos metálicos que nos escanean parecen sugerir una seguridad mayor minimizando la presencia de armas en el interior de edificios, aviones, trenes, etc. Pero ¿seguirán siendo útiles cuando un criminal o terrorista tan sólo necesite acceder a una impresora 3D ubicada en un edificio oficial y, usando unos planos guardados en una memoria USB, pueda «construir» un arma en pocas horas?

Estas impresoras son cada vez más rápidas, potentes y comunes. Las impresoras 3D industriales podrían imprimir mucho más que una simple pistola. La percepción de seguridad cambia a media que la tecnología avanza.

Los terroristas, los piratas, los hackers o, simplemente, los delincuentes comunes celebran más que tú y que yo los avances tecnológicos. Los ven como una oportunidad que, además, abre su espectro y garantiza más su impunidad. Salir con un fusil disparando gente por las calles de París tiene un final de aventura previsible. Estar en un hotel con un ordenador perpetrando alguna barbaridad a cientos o miles de kilómetros de distancia no requiere ese desgaste físico y ese riesgo personal.

La privacidad es definitivamente cosa del pasado, y la seguridad de las personas podría verse comprometida por culpa de esa misma tecnología que nos maravilla, y en la que estamos dispuestos a gastar ingentes cantidades de dinero todos los años.

Es la paradoja del mundo contemporáneo. La dicotomía del mundo anterior a la caída del muro de Berlín era una elección entre la libertad que ofrecía Occidente y la seguridad de la que se vanagloriaba el bloque comunista, un dilema que expresó en una ocasión el expresidente Felipe González cuando afirmó: «Prefiero morir apuñalado en el metro de Nueva York que de aburrimiento en Moscú». Pues bien, ese antiguo dilema entre libertad y seguridad se ha evaporado para siempre.

En el futuro hiperconectado que nos aguarda, la libertad y la seguridad dejarán de ser opciones, y serán sacrificadas en aras del progreso técnico. Pero tampoco nos conviene preocuparnos más de la cuenta; al fin y al cabo, no hay nada que podamos hacer para detener la revolución tecnológica. Hemos sobrepasado el punto de no retorno, y ya no hay vuelta atrás. Así que renueva tu antivirus y relájate. Puedes seguir jugando a Angry Birds, actualizar tu estado de Facebook o salir a correr con tu pulsera Fitbit. Mañana volverá a salir el sol. Y el sol no se puede hackear. De momento, pero yo no pondría por siempre la mano en el fuego.

Entramos en una guerra fría tecnológica entre dos bloques bien diferenciados. Los que usan la tecnología para el bien y los que

aprenderán de dichos avances adaptándolos para ejercer el mal; estos últimos irán generando nuevos problemas y amenazas que no estaban antes en nuestra hoja de ruta.

Llegan nuevos tiempos de incertidumbre y amenazas nunca antes imaginadas. Suerte, amigo. Toda precaución será poca.

# Bibliografía


Adams, James, *La próxima guerra mundial: los ordenadores son las armas y el frente está en todas partes*, Ediciones Granica, Buenos Aires, 1999.

Deibert, Ronald J., *Black code: surveillance, privacy, and the dark side of the Internet*, Signal, Toronto, 2013.

García Mostazo, Nacho, *Libertad vigilada: el espionaje de las comunicaciones*, Ediciones B, Barcelona, 2003.

Goodman, Marc, *Future crimes: everything is connected, everyone is vulnerable and what we can do about it*, Doubleday, Nueva York, 2015.

Greenwald, Glenn, *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*, Metropolitan Books/Henry Holt, Nueva York, 2014.

Javers, Eamon, *Broker, Trader, Lawyer, Spy: inside the secret world of corporate espionage*, Harper, Nueva York, 2010.

Pasquale, Frank, *The black box society: the secret algorithms that control money and information*, Harvard University Press, Cambridge (Massachusetts), 2015.

Peirano, Marta, *El pequeño libro rojo del activista en la red*, Roca, Barcelona, 2015.

Singer, Peter W., y Allan Friedman, *Cybersecurity and cyberwar: what everyone needs to know*, Oxford University Press, Nueva York, 2014.

Stel, Enrique, *Seguridad y defensa del ciberespacio,* Editorial Dunken, Buenos Aires, 2014.

# Notas

[1]. La norma X.25 se define como la interfaz entre equipos terminales de datos y equipos de terminación del circuito de datos para terminales que trabajan en modo paquete sobre redes de datos públicas.

[2]. Economista austriaco de origen judío que planteó lo perjudicial del poder y de la intervención gubernamentales en la economía, ya que, según su teoría, por lo general llevan a un resultado distinto al natural y, por ello, a menudo perjudicial para la sociedad, ya que generan caos en el largo plazo.

[3]. El *kohl* es un cosmético a base de galena molida y otros ingredientes, usado principalmente por las mujeres de Oriente Medio, Norte de África, África subsahariana y sur de Asia, y, en menor medida, por los hombres, para oscurecer los párpados y como máscara de ojos.

[4]. En el islam, pronunciamiento legal emitido por un especialista en ley religiosa sobre una cuestión específica.

[5]. Carl Philipp Gottlieb von Clausewitz fue un militar prusiano, y uno de los más influyentes historiadores y teóricos de la ciencia militar moderna.

*El quinto elemento*
Alejandro Suárez

No se permite la reproducción total o parcial de este libro, ni su incorporación a un sistema informático, ni su transmisión en cualquier forma o por cualquier medio, sea éste electrónico, mecánico, por fotocopia, por grabación u otros métodos, sin el permiso previo y por escrito del editor. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (Art. 270 y siguientes del Código Penal)

Diríjase a CEDRO (Centro Español de Derechos Reprográficos) si necesita reproducir algún fragmento de esta obra.
Puede contactar con CEDRO a través de la web www.conlicencia.com o por teléfono en el 91 702 19 70 / 93 272 04 47

© del diseño de la portada, microbiogentleman.com, 2015
© de la imagen de la portada, Anton Seleznev - Getty Images

© Alejandro Suárez, 2015

© Centro Libros PAPF, S. L. U., 2015
Deusto es un sello editorial de Centro Libros PAPF, S. L. U.
Grupo Planeta, Av. Diagonal, 662-664, 08034 Barcelona (España)
www.planetadelibros.com

Primera edición en libro electrónico (epub): octubre de 2015

ISBN: 978-84-234-2195-4 (epub)

Conversión a libro electrónico: Àtona - Victor Igual, S.L.
www.victorigual.com